UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

ANALISIS COMPARATIVO ENTRE SISTEMAS OSSTMM Y COBIT 5.0 PARA LA MITIGACION DE RIESGOS

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Edgard Eliecer Molina Vega
Profesor Guía : Roberto Caru Cisternas

Santiago – Chile
Agosto, 2016

AGRADECIMIENTOS

Doy gracias a Dios por la ayuda brindada en este tiempo que cuando vea esta memoria los traerá a mi mente, pasé por momentos difíciles pero con perseverancia, buenos compañeros, amigos y la comprensión y ayuda de mis profesores puedo decir con alegría que concluí una etapa importante de mi vida.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1 INTRODUCCION

La seguridad informática, que contempla en la actualidad un importante número de disciplinas y especialidades distintas y complementarias, se ha convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de los países.

Las empresas tienen la responsabilidad de asegurarse que sus trabajadores sigan pasos adecuados en la línea de la protección y defensa. Es cierto que estos protocolos son sencillos de romper, pero también son sencillos de usar. Por ejemplo, no supone un gran esfuerzo pensar en contraseñas no muy simples, o no utilizar la misma contraseña para las distintas aplicaciones de las que dispone, esto por si alguien robara su contraseña, no tendrá oportunidad de acceder con ella a toda su información.

Si empezamos por admitir que el objetivo es mantener los sistemas informáticos disponibles y funcionando, entonces, si no lo están, el costo de esto es una pérdida tangible y en muchos casos intangible pero igual de dispendioso, como sería el caso de la reputación de un banco.

La principal motivación, radica en el hecho de presentar con datos reales, la importancia que tiene el activo que representa la información en las empresas.

El mundo se globaliza en los negocios y también en las amenazas. Al mismo tiempo, las empresas dependen cada vez más de los datos generados por y para su negocio y la consecuente información que estos generan. Obtener el nivel de seguridad deseado es todo un reto: amenazas que evolucionan vertiginosamente, tecnologías que cambian día a día, redes que se complejizan más y más.

Dadas las condiciones actuales en la red mundial, es imprescindible hacer algo al respecto para de alguna manera evitar cualquier tipo de amenazas a los activos de esta entidad. El departamento de informática del Gobierno autónomo Descentralizado Municipal de Santa Ana de Cotacachi tiene las soluciones tradicionales de firewall y antivirus que son necesarias para evitar la transferencia de programas malintencionados, pero no son suficientes para combatir la nueva generación de amenazas y ataques dirigidos. Tampoco los usuarios y empleados que dan uso a diario de los activos y de la red interna, poseen una cultura de seguridad que pueda salvaguardar la información almacenada en formato electrónico.

2 PLANTEAMIENTO DEL PROBLEMA

Las empresas deben contar con una infraestructura tecnológica lo más actualizada posible, además debe ser lo suficientemente robusta para atender todos los requerimientos que los clientes necesiten, ya que cada día es más fácil tener accesos a sistemas informáticos que faciliten las actividades diarias, lo cual ha venido cambiando aceleradamente en los últimos años. Hoy, los usuarios son más exigentes y tienden a preferir los servicios tecnológicos y por ende a las empresas que se encuentren más actualizadas tecnológicamente. Las empresas en Chile, no escapan a los avances tecnológicos, ya que en este país el acceso a la tecnología es bastante alto, lo que coloca a las empresas a la dependencia en un alto grado del uso de tecnología de la información que ofrecen al público, su infraestructura tecnológica es lo suficientemente robusta y actualizada para prestar de manera ágil los servicios a sus clientes, por lo que en las empresas en Chile, se hace necesario gestionar adecuadamente el riesgo tecnológico, para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios.

Actualmente, las grandes empresas en Chile cuenta con planes de recuperación de desastres, planes de contingencia, infraestructura tecnológica dual y ya ha realizado eventos de contingencia, pero muy pocas de ellas aún no cuenta con indicadores que le permitan definir tiempos de recuperación y cuál es el grado de madurez que se ha alcanzado en la mitigación del impacto del riesgo tecnológico, lo cual coloca a la instituciones en un nivel de riesgo muy alto, además de incumplir con la normativas de riesgo tecnológico.

Es por ello en consecuencia, las organizaciones experimentan la necesidad de definir estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle mayor resguardo a la información, y al mismo tiempo no obstáculos para adaptarse a los continuos cambios de la organización como consecuencia de las exigencias del mercado.

2.1 Pregunta de Investigación

¿Cuál deberá ser la metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos?

2.2 Objetivo General

- Generar un análisis comparativo entre el uso de metodología OSSTMM o sistema COBIT 5.0, para medir los impactos en riesgos tecnológicos.

2.3 Objetivos Específicos

- Análisis la importancia de la seguridad informática.
- Analizar el uso de la metodología OSSTMM
- Analizar el uso de la metodología COBIT 5.0
- Determinar el impacto de los peligros en distintos escenarios en función del riesgo asociado a la línea de negocio, por medio de la identificación del riesgo inherente y el riesgo residual.

3 MARCO TEORICO

3.1 Introducción

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar las operaciones, reduciendo significativamente el uso del papel, a su vez reduciendo los costos al compartir información. Sin embargo, el éxito de muchos de estos esfuerzos depende, en gran parte, de la capacidad de la organización para proteger la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos. Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la seguridad de la información debe convertirse en una de las principales preocupaciones de una empresa.

La seguridad de la información ha sido un área de investigación durante mucho tiempo. Inicialmente los virus y los gusanos se propagaban lentamente a través del intercambio de contenedores magnéticos como los disquetes. Con el desarrollo del internet, los problemas de seguridad se han hecho más frecuentes y han tomado formas muy diferentes, dando lugar al desarrollo de las técnicas nuevas de seguridad. Los principios básicos clásicos de la seguridad de la información, que son, la confidencialidad, integridad y disponibilidad, constituyen la base para su protección de la TI[1] . Los términos tecnología de información y comunicaciones, y tecnología de información y telecomunicaciones se utilizan con frecuencia como sinónimos. Debido a

[1] Tecnología de la Información hace referencia a los dispositivos que almacenan, procesan, transmiten, convierten, copian o reciben información electrónica.

la longitud de estas expresiones, se han establecido abreviaturas y por lo tanto la gente en general, simplemente se refiere a ella como TI.

3.2 Importancia de la seguridad informática

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad está garantizada. En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto necesita ser protegido adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio han vuelto más comunes, y cada vez son más sofisticadas. (Norma ISO 27001, 2005)

La seguridad de la información a más de ser un problema de TI, también es un asunto de negocios. Si una empresa quiere sobrevivir, y mucho más prosperar, es necesario comprender la importancia de la seguridad de la información y poner en práctica medidas y procesos apropiados. Es vital estar preocupado por la seguridad de la información ya que gran parte del valor de una empresa se concentra en el valor de su información. La información es la base de la ventaja competitiva[2] de las empresas. Tanto en el sector privado como en el sector público, se debería tener mayor conciencia de la probabilidad de robo de identidad y en sí de la información. Sin información, ni las empresas privadas ni públicas podrían funcionar. Por tanto valorar y proteger la información son tareas cruciales para las organizaciones modernas.

[2] Son ventajas que posee una empresa ante otras empresas del mismo sector o mercado, que le permite destacar o sobresalir ante ellas, y tener una posición competitiva en el sector o mercado.

La razón básica acerca de los sistemas de seguridad, es que la información confidencial de una empresa debe ser protegida contra la divulgación no autorizada, por motivos ya sea confidencial o competitivo; toda la información que se almacena también debe ser protegida contra la modificación accidental o intencionada y a su vez debe estar disponible de manera oportuna. Además hay que establecer y mantener la autenticidad de los documentos que las organizaciones crean, envían o reciben.

Otro tema de la importancia de la seguridad informática, es el comercio electrónico que se puede ver como parte de la estrategia de desarrollo del mercado. Los consumidores han expresado su preocupación general por la privacidad y la seguridad de sus datos, las empresas con una fuerte seguridad pueden aprovechar su inversión para aumentar el número de compradores y a su vez aumentar su cuota de mercado. Ya no se tiene que mirar a la seguridad informática únicamente como para evitar la pérdida de la información, la seguridad informática hoy se convierte en una ventaja competitiva que puede contribuir de manera directa a las cifras de ingresos y así el progreso de una empresa.

3.3 Principios importantes de la seguridad informática

La seguridad informática se basa en la confidencialidad, integridad, disponibilidad y autenticación. Las interpretaciones de estos cuatro aspectos pueden variar de acuerdo al entorno pero básicamente se relaciona con la protección de las amenazas a la seguridad del sistema.

3.3.1 Confidencialidad

En el contexto de seguridad de la información, la confidencialidad significa que la información que debe permanecer en secreto y sólo aquellas personas autorizadas a la información, pueden recibir el acceso. El acceso no autorizado a la información

confidencial puede tener consecuencias devastadoras, no sólo en aplicaciones de seguridad nacional, sino también en el comercio y la industria. Los principales mecanismos de protección de la confidencialidad en los sistemas de información son los controles de acceso y criptografía, como ejemplo de las amenazas a la confidencialidad se tiene los malware, los intrusos, la ingeniería social, las redes inseguras, y los sistemas mal administrados

3.3.2 Integridad

La integridad se refiere a la confiabilidad, el origen, y la exactitud de la información, así como la prevención de la modificación indebida o no autorizada de la información. La integridad en el contexto de seguridad de información no sólo se refiere a la integridad de la información en sí, sino también a la integridad de origen, es decir, la integridad de la fuente de información. Los mecanismos de protección de integridad se pueden agrupar en dos grandes tipos: los mecanismos preventivos, como los controles de acceso que impiden la modificación no autorizada de la información y los mecanismos detectives, que están destinados a detectar modificaciones no autorizadas cuando los mecanismos de prevención han fallado. (Guzmán, 2011)

3.3.3 Disponibilidad

La disponibilidad se refiere a la capacidad de utilizar la información o el recurso deseado en cualquier momento determinado. La disponibilidad es un aspecto importante de fiabilidad, ya que un sistema no disponible es igual a no tener ningún sistema. El aspecto de la disponibilidad puede verse comprometido por alguien quien puede deliberadamente hacer arreglos para negar el acceso a los datos o a un servicio, al hacer que este no esté disponible. Alguien puede ser capaz de manipular los recursos, o el tráfico de red, esto significa que los mecanismos para mantener el recurso o los datos disponibles, no trabajan en un entorno para el que no fueron diseñados. Como resultado, a menudo se producirá un error (Sánchez, 2009, p. 102).

3.3.4 Autentificación

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite garantizar el acceso a los recursos únicamente a las personas autorizadas, gracias a una contraseña codificada.

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

3.4 Modelos de seguridad

3.4.1 Seguridad por oscuridad

Es uno de los primeros modelos de seguridad que se aplicó en el campo informático, es denominado seguridad por oscuridad, porque está basada en el desconocimiento u ocultamiento de lo que se desea proteger, en este caso son los recursos informáticos; este modelo funciona mientras realmente permanezca secreto u oculto, es decir que en la práctica puede funcionar por un tiempo limitado, porque a largo plazo se va a descubrir y su seguridad posiblemente va a ser violentada. (Eleclibre. 2011)

3.4.2 Perímetro de defensa

Proteger el perímetro de la red es quizá lo más razonable para mantener a salvo la información y los sistemas de una red de los ataques externos. De esta manera se está separando la red interna con la red externa con el único fin de proteger todos los puntos de acceso a la red, lo que es correcto y en la actualidad se mantiene (Eleclibre. 2011).

Los problemas principales de este modelo son: que no brinda seguridad frente a los ataques que se realicen desde la red interna y que no presenta un nivel de protección en caso de que el ataque rompa la barrera de seguridad perimetral (Sánchez, 2009, 101)

3.4.3 Defensa en profundidad

Defensa en profundidad es el uso coordinado de las contramedidas de seguridad múltiples para proteger la integridad de los activos de información de una empresa. La estrategia se basa en el principio militar, es más difícil para un enemigo derrotar a un sistema de defensa complejo y de múltiples capas que penetrar una sola barrera. La defensa en profundidad minimiza la probabilidad de que los esfuerzos de los hackers tengan éxito. Una estrategia bien diseñada de este tipo también puede ayudar a los administradores de sistemas informáticos y personal de seguridad a identificar a las personas que tratan de comprometer un ordenador, servidor o una red. Si un hacker quiere acceder a un sistema, la defensa en profundidad reduce al mínimo el impacto adverso y proporciona a los administradores e ingenieros un tiempo de implementación de contramedidas nuevas o actualizadas para prevenir la recurrencia.

Los componentes de la defensa en profundidad incluyen el software antivirus, cortafuegos, programas anti-spyware[3] , contraseñas jerárquicas, detección de intrusos y verificación biométrica. Además de las contramedidas electrónicas, la protección física de los recursos, junto con la capacitación del personal integral y continuo mejora la seguridad de los datos de cualquier peligro, robo o destrucción.

3.5 Ataques comunes basados en el modelo TCP/IP

En base al modelo TCP/IP compuestas por 4 capas que son: Acceso a red, Internet, Transporte y Aplicación se puede realizar un enfoque general de las vulnerabilidades de cada capa, las cuales se detallan a continuación.

3.5.1 Capa acceso a RED

Los principales inconvenientes en esta capa pueden ocurrir en la administración de enlace de datos y en la transmisión física de datos en los medios, esto tiene que ver el acceso a los equipos con los que la red opera, el acceso al cuarto de telecomunicaciones, al cableado o a los dispositivos remotos establecidos para la comunicación; también presenta vulnerabilidades en el transporte del mensaje de origen al destino, el mensaje puede sufrir de ataques de intrusos como modificación, o eliminación. A continuación se detalla las amenazas más comunes que puede suceder en la capa acceso a red.

[3] Es un eliminador de programas espías que recopilan información sobre una persona u organización sin su conocimiento

3.5.1.1 Amenaza a las instalaciones

Las amenazas a las instalaciones pueden darse por diferentes motivos como por ejemplo.

- Carencia del perímetro de seguridad
- Si cualquier usuario puede acceder a todas las oficinas de la empresa, sin controles ni barreras físicas, es muy probable que acceda un intruso a las instalaciones provocando actos ilícitos como hurtos, daños físicos o espionaje de información confidencial
- Falta de barreras físicas que protejan los activos Si no se establece un perímetro de seguridad, la empresa se convierte en una continuación física de la vereda;
- Falta de áreas protegidas que guarden los equipos críticos Permitiendo el acceso indiscriminado de personas.
- Falta de autenticación de usuarios. Esto dificulta la identificación de usuarios no autorizados.
- Ausencia de métodos confiables de autenticación de usuarios. Un método no confiable de autenticación de usuarios es levemente mejor que ningún método de autenticación de usuarios.
- Señalización indiscreta del edificio o sobre indicación. La ayuda que se da para acceder a los sectores protegidos será una herramienta útil para un intruso que desee perpetrar las instalaciones.
- Hacer pública información sensible. Toda información delicada debe ser cuidadosamente administrada, pues todo dato es una llave para el sistema, que un intruso experimentado puede utilizar (Victoria, 2011)

3.5.1.2 Amenazas por interceptación intrusiva en los mensajes por el uso de una red física

Cuando un mensaje (M) es enviado por un usuario origen (X) a un usuario destino (Y) determinado a través de una red, este mensaje viaja por el medio físico con el riesgo de sufrir alguno de los siguientes ataques por parte de un intruso (I) (Bisogno, 2004)

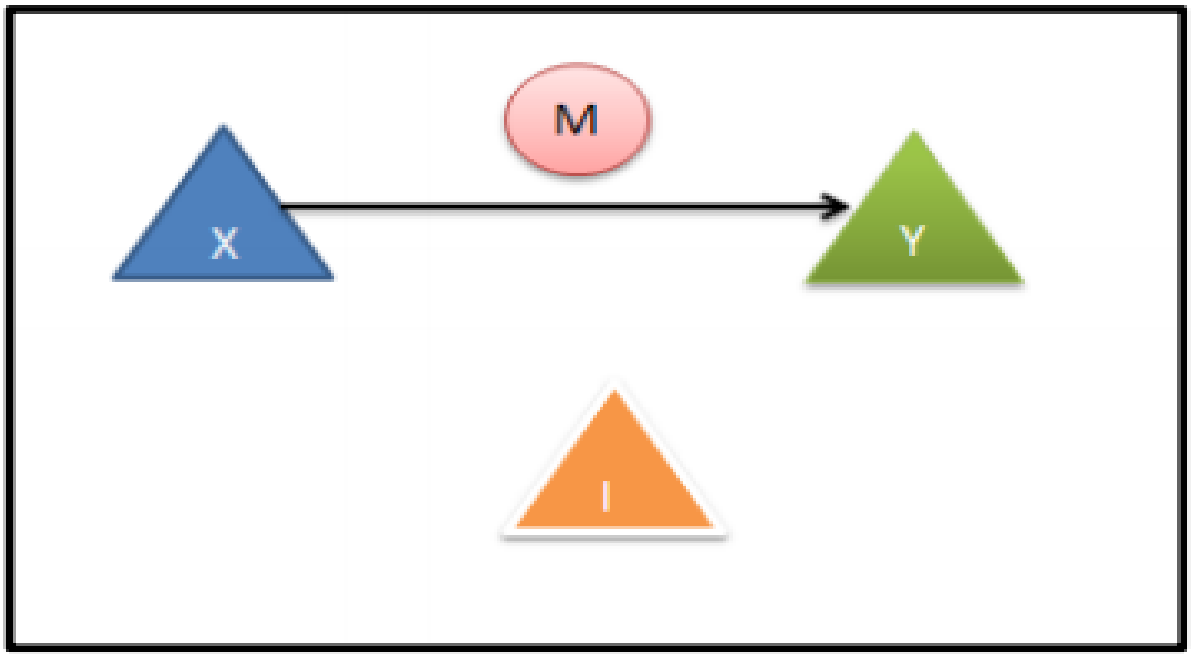


Figura 3-1[4]

Elementos de una red Física.

Mensaje (M), Origen (X), Destino (Y), Intruso (I).

[4] Recuperado de: Tesis de grado (Bisogno, 2004)

3.5.1.2.1 Interrupción

Sucede cuando el destinatario nunca recibe el mensaje emitido por el origen:

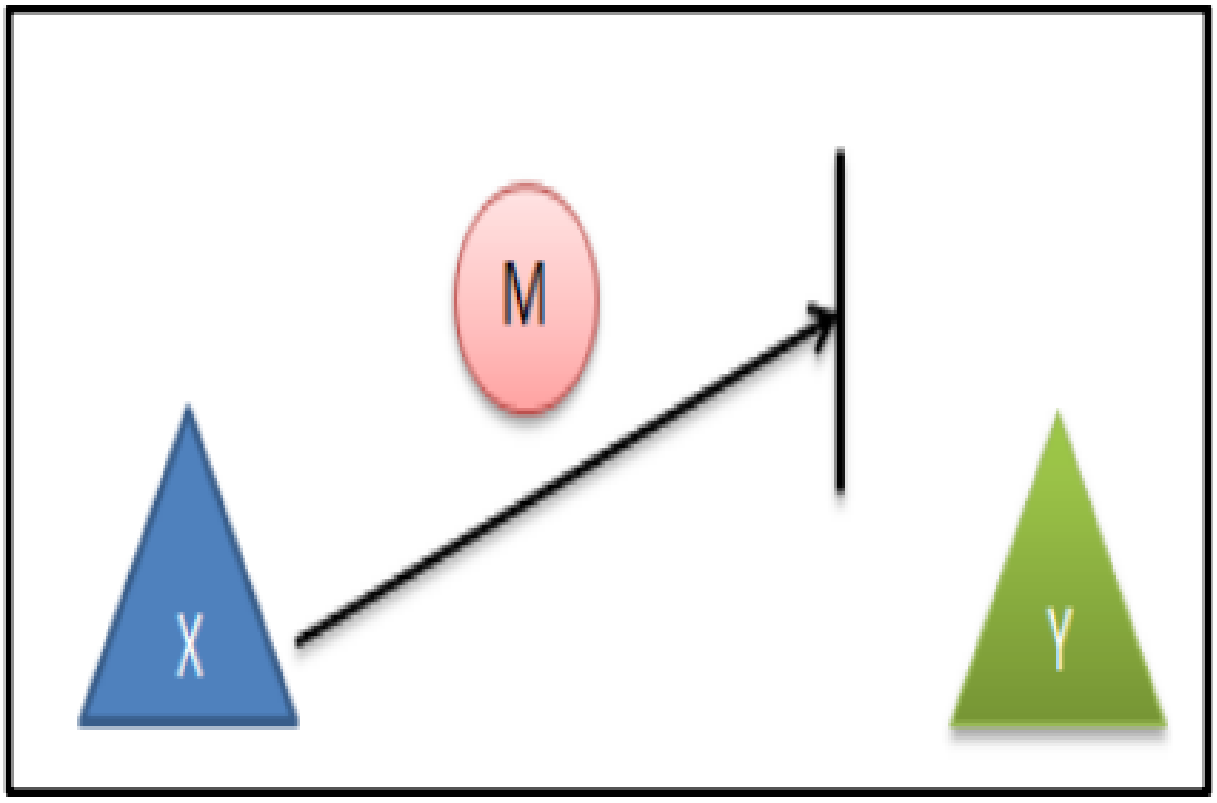


Figura 3-2.[5]

Interrupción de un mensaje.

[5] Recuperado de: Tesis de grado (Bisogno, 2004)

3.5.1.2.2 Intercepción

El mensaje enviado por el origen es interceptado por un intruso que recibe el mensaje tanto como el verdadero destino

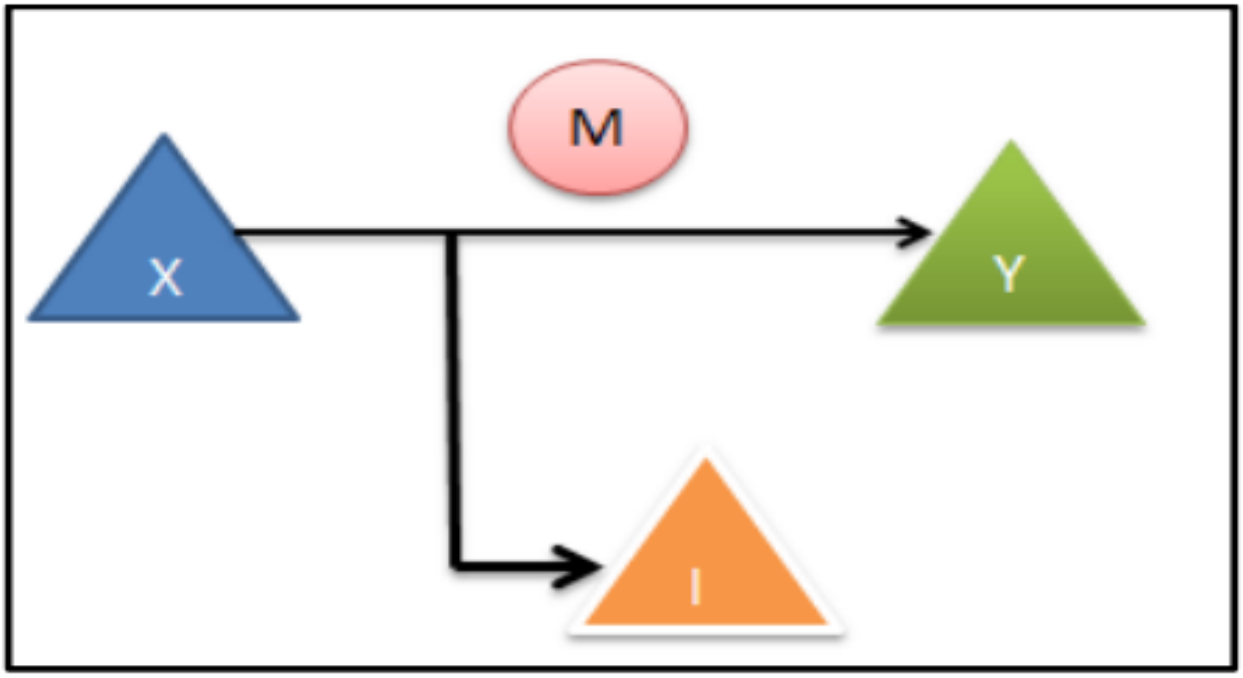


Figura 3-3.
Intercepción de un mensaje.[6]

[6] Recuperado de: Tesis de grado (Bisogno, 2004)

3.5.1.2.3 Modificación

El mensaje enviado por el origen es interceptado por un intruso que lo modifica, y lo reenvía modificado al verdadero destino. El destino recibe el mensaje modificando creyendo que es el original

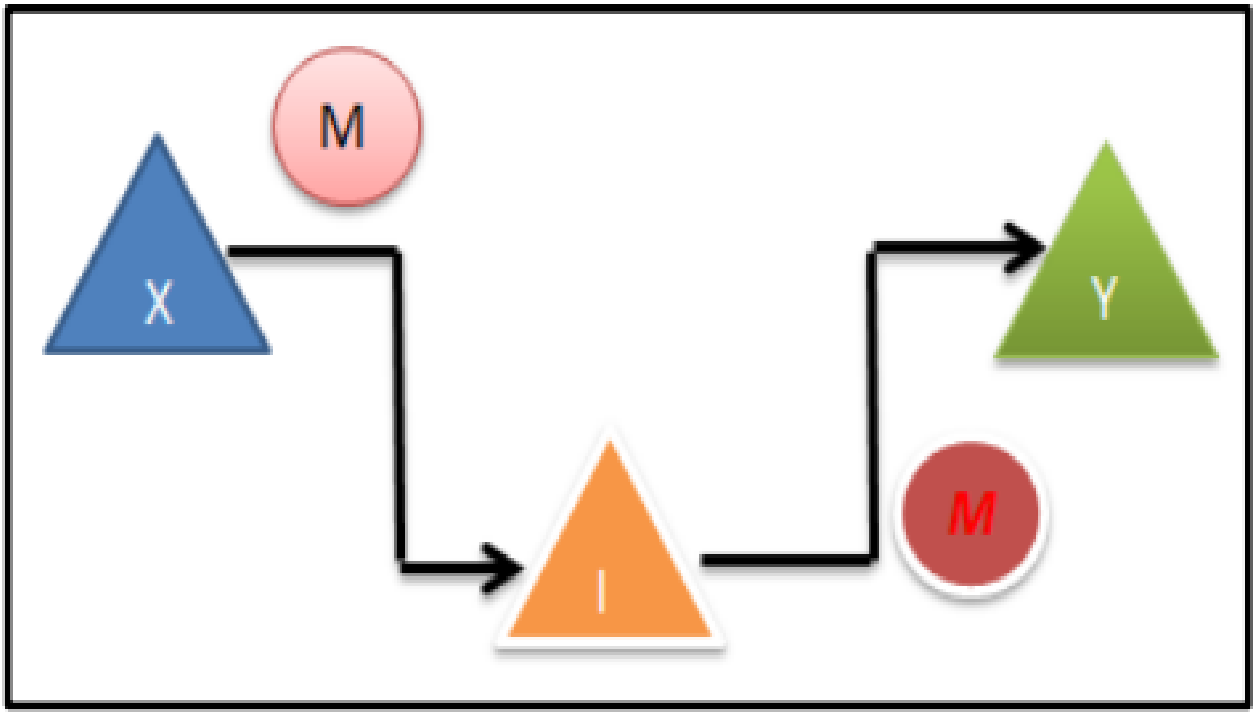


Figura 3-4:[7]

Modificación de un mensaje.

[7] Recuperado de: Tesis de grado (Bisogno, 2004)

3.5.1.2.4 Fabricación

El mensaje enviado por el origen nunca es distribuido; en su lugar el intruso envía otro mensaje en reemplazo del original

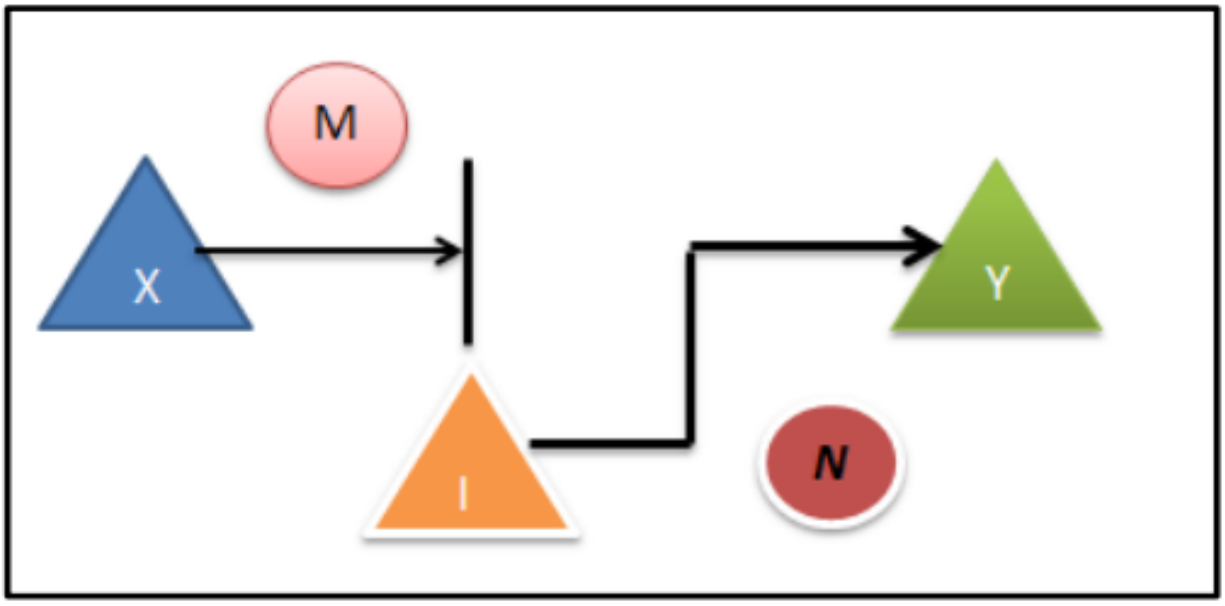


Figura 3-5.

Fabricación de un mensaje. [8]

3.5.2 Capa INTERNET

Es la capa de donde mayor información se puede obtener para vulnerar un sistema. Lo primordial para permitir a ésta es tener acceso a los datagramas IP los que se pueden encontrar en cada paquete que circula por la red, mediante Softwares espías. Estos Softwares permiten recolectar información mediante un proceso que se conoce como Sniffing.(Riffo, 2009)

[8] Recuperado de: Tesis de grado (Bisogno, 2004)

3.5.2.1 Técnicas de sniffing

En su forma simple un sniffer captura todos los paquetes de datos que pasan a través de una interfaz de red dada. Normalmente, el sniffer sólo capturar los paquetes que estaban destinados a la máquina en cuestión. Sin embargo, si se coloca en modo promiscuo[9], el analizador de paquetes también es capaz de capturar todos los paquetes que atraviesan la red, independientemente del destino.

Al colocar un sniffer en una red en modo promiscuo, un intruso malicioso puede capturar y analizar todo el tráfico de red. Dentro de la red puede encontrar información, como el nombre de usuario y la contraseña que generalmente es transmitida en una sesión. Un sniffer sólo puede capturar paquetes de información dentro de una subred determinada. Por lo tanto, no es posible para un atacante malicioso colocar un sniffer de paquetes en su casa para el ISP de la red y capturar el tráfico de red desde su subred (Jauregui, 2009) Entre los programas sniffers más conocidos están: SpyNet, Ethereal, WinSniffer.

3.5.2.2 Falsificación de direcciones IP

La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Por ejemplo, el popular ataque smurf[10] hace uso de una característica de los enrutadores (routers) para enviar una secuencia de paquetes a miles de máquinas. Cada paquete contiene una dirección IP de origen que es suplantada de una víctima. Las máquinas a las que estos paquetes falsificados son enviados inundan a la máquina víctima generalmente deteniendo sus servicios o bien deteniendo los servicios de una red completa.

[9] Se refiere a una computadora conectada a una red, la cual captura todo el tráfico de la red y no solo el tráfico destinado a la misma.
[10] Técnica de ataque haciendo uso de la falsificación de ip

3.5.3 Capa transporte

La principal tarea de la Capa de Transporte es proporcionar la comunicación entre un programa de aplicación y otro, transmite información TCP o UDP sobre datagramas IP. Las principales vulnerabilidades están asociadas a la denegación de servicio, intercepción de sesiones TCP con el objetivo de secuestrarlas y dirigirles a otros equipos con fines deshonestos. Estos términos se relacionan con el acceso a los protocolos de comunicación entre capas, permitiendo la denegación o manipulación de ellos (Daniel, sf)

3.5.3.1 Desviación del tráfico

La posibilidad de interceptar conexiones TCP abierta, llamada también secuestro de conexiones TCP, es operada generando paquetes TCP con fines malignos que encajen en el flujo de una conexión ya establecida. También puede darse debido a la poca exigencia en cuanto a autenticación de los equipos en comunicación. (Seguridad en Redes, 2010)

3.5.3.2 Denegación de Servicio (DDoS)

Los ataques de denegación de servicio a nivel de transporte se deriva de los errores en algunas implementaciones de la pila Tcp/ip. La denegación de servicio en muchos casos es debido a las esperas llamadas time-outs del protocolo de establecimiento de conexión. Otra manera de generar denegación de servicio es iniciar conexión SYN y no responder al asentimiento SYN-ACK dejando en espera al otro extremo (Paz, 2010)

3.5.3.3 Desbordamiento de Buffer

Los ataques por desbordamiento de búfer también denominado saturación de búfer, están diseñados para activar la ejecución de un código arbitrario en un programa al enviar un caudal de datos mayor que el que puede recibir, es decir se produce cuando la entrada de un sistema es mayor que el área de memoria asignada para contenerla buffer y el sistema no lo comprueba adecuadamente. (Kioskea, 2012)

3.5.4 Capa aplicación

Permite a las aplicaciones acceder a los servicios que ofrecen las demás capas. Cada aplicación tiene sus propios protocolos, con lo que sería imposible enumerarlos a todos, pero hay unos protocolos claros y estándar para este nivel como son: DNS, Telnet, HTTP y FTP.

3.5.4.1 Servicio de nombres de dominio

Se encarga de generar las solicitudes de cada usuario que circulan por la red, es decir, en el momento que una persona solicita una conexión a un servicio determinado, se solicita una dirección IP y un nombre de dominio, se envía un paquete UDP a un servidor DNS. Lo que hace el servidor DNS es responder a ésta solicitud y entregar los datos que fueron pedidos, éste servidor DNS funciona como una base de datos en donde se encuentran las direcciones que solicitan los usuarios, por lo tanto, cuando se tiene acceso a esta base de datos se presenta un inconveniente, el cual hace vulnerable al sistema, ya que puede ser modificada a gusto de la persona que le quiere sacar provecho a esa información, pudiendo entregar direcciones incorrectas o receptar las peticiones de los usuarios para obtener información acerca de sus cuentas. (Apaza, 2011)

3.5.4.2 Telnet

Normalmente, el servicio telnet autentica al usuario mediante solicitud de identificador de usuario y su contraseña que se transmiten en claro por la red, así al igual que el resto de servicios de internet que no protegen datos por medios de protección, el protocolo de aplicación de Telnet hace posible la captura de aplicación sensible, mediante el uso de técnicas de sniffing.

3.5.4.3 File Transfer Protocol

Al igual que Telnet también envía la información sin protección, con lo cual también queda expuesto de la misma forma que el anterior. Este servicio también permite el acceso anónimo, aunque por lo general esta forma de conexión solo permite el acceso a una zona restringida en la cual solo se permite la descarga de archivos. (Jiménez, sf)

3.5.4.4 Hypertext Transfer Protocol

Está dado por el protocolo HTTP, el cual es responsable del servicio World Wide Web. La principal vulnerabilidad de este protocolo, está asociado a las deficiencias de programación que puede presentar un link determinado, lo cual puede poner en serio riesgo el equipo que soporta este link, es decir, el computador servidor.

La secuencia de comandos de sitios Una de las principales vulnerabilidades es la secuencia de comandos en sitios cruzados, más conocida como XSS[11]. Diego dice XSS es la más prevaleciente y perniciosa problemática de seguridad en aplicaciones Web. Las fallas de XSS ocurren cuando una aplicación toma información originada por un usuario y la envía a un navegador Web sin primero validarla o codificando el contenido. XSS permite a los atacantes ejecutar secuencias de comandos en el navegador Web de

[11] Es un subconjunto de inyección HTML que consiste en re-direccionar una página a otra que se haya designado.

la víctima, quienes pueden secuestrar sesiones de usuario, modificar sitios Web, insertar contenido hostil, realizar ataques de phising[12] , y tomar control del navegador Web del usuario utilizando secuencias de comando maliciosas. Generalmente JavaScript es utilizado, pero cualquier lenguaje de secuencia de comandos soportado por el navegador de la víctima es un potencial objetivo para este ataque.

3.6 Auditoria de seguridad informática

3.6.1 Introducción

Con la explotación en el uso del Internet en los últimos 10 años, tanto las empresas grandes como las pequeñas, se han visto obligadas en asegurar su componente vital que es la tecnología de la información. Actualmente las empresas, cuenta con el valioso recursos de TI, tales como computadoras, redes de datos, sistemas informáticos, etc. Para la protección de los activos de una empresa, se sugiere que haya tenido al menos una auditoría de seguridad, con el fin de obtener una imagen clara de los riesgos de seguridad que enfrentan y saber la mejor manera de tratar con esas amenazas. El propósito de una auditoría de seguridad no es para culpar o desmerecer el diseño de una red, sino para garantizar la eficacia, integridad y el cumplimiento de las políticas de seguridad de la empresa. La auditoría ofrece la habilidad de probar los sistemas, encontrar riesgo y comprobar si los controles son los apropiados para mitigar la exposición a los diferentes riesgo, cabe recalcar que la auditoría de seguridad no sólo trata de cómo ejecutar un sin número de herramientas de hackers, en un intento de entrar en la red.

[12] Es una página web donde se simula suplantando visualmente la imagen de una entidad oficial, pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la imitación de páginas web de bancos, siendo el parecido casi idéntico pero no oficial.

Hay muchos tipos de auditoría y el alcance de una auditoría define lo que el auditor desea inspeccionar y con qué frecuencia. Muchas organizaciones requieren una auditoria externa anual, mientras que otras necesitan auditorías internas cada seis meses, después de cualquier gran proyecto de TI. (La auditoría como actividad profesional, 2010) El beneficio final de la auditoría es mejorar continuamente el procedimiento de los procesos y controles establecidos para asegurar los activos valiosos de la empresa, ya que las mismas hoy en día tienen una responsabilidad con sus clientes para salvaguardar sus datos confidenciales.

3.6.2 Objetivo fundamental de la auditoria informática

La Auditoria de seguridad Informática se la puede definir como el conjunto de procedimientos y técnicas para evaluar y controlar la tecnología de la información con el fin de verificar si los recursos encargados de salvaguardar la información están operando de manera correcta. El Objetivo fundamental de la auditoria de seguridad informática es de mejorar la rentabilidad, la seguridad y la eficacia del sistema, mediante la exposición de las debilidades y disfunciones, que se van encontrando en el proceso, para luego levantar un informe final donde se indique los planes de acción para eliminar dichas falencias a modo de recomendaciones.

3.6.3 Características de la auditoria de seguridad informática

- La auditoría es sistemática esto quiere decir que los resultados obtenidos son debidos a un análisis meticuloso, metódico y planificado por parte del auditor, que garantiza un grado de fiabilidad.

- La auditoría es totalmente independiente ya que es imposible para una empresa autoevaluarse en forma objetiva.

- Evalúa si las acciones preventivas tendentes al control de los riesgos de ataques o falencias detectados en la empresa, son eficaces o no, en función de los resultados obtenidos.

- La auditoría se encarga de analizar el estado actual de la empresa para dar soluciones a futuro, sin la necesidad de encontrar un culpable de las posibles falencias de la tecnología de la información (Martínez, 2009)

Las características se las puede resumir gráficamente en este esquema.

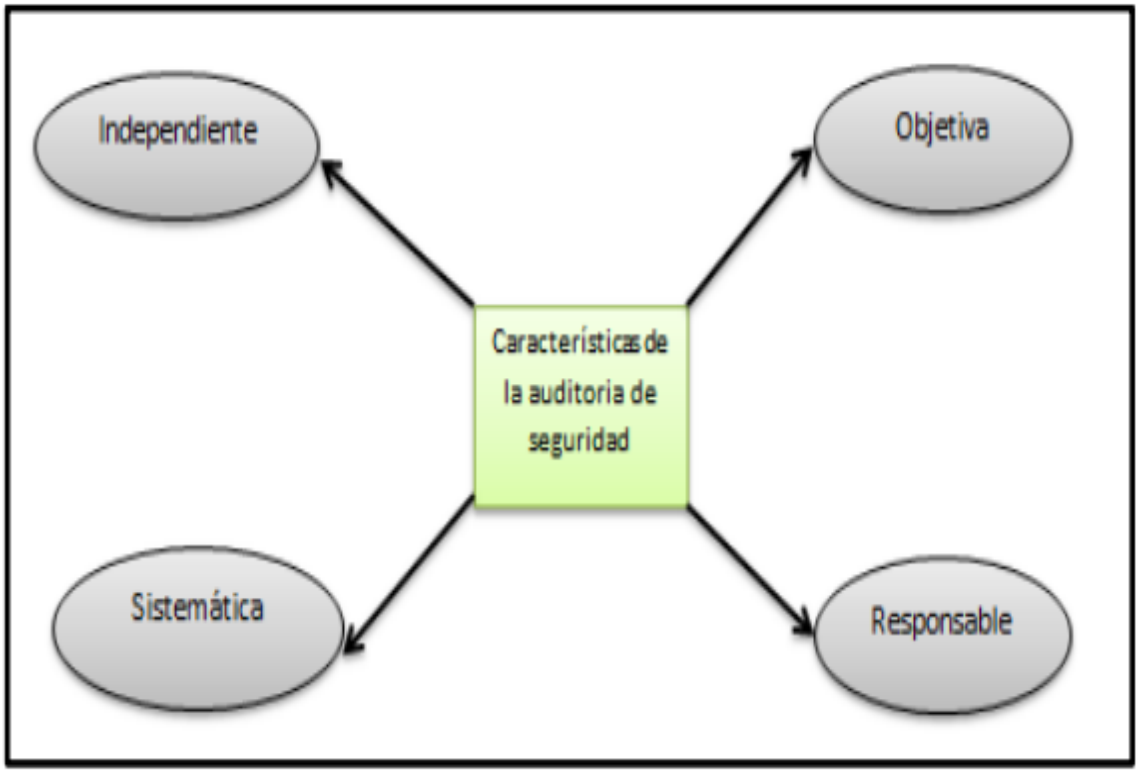


Figura 3-6:
Características de la auditoría de seguridad informática

3.6.4 Síntomas de necesidad de una auditoria de seguridad informática

- Síntomas de mala imagen e insatisfacción de los usuarios:

No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario. No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario observa que está abandonado y desatendido permanentemente.

- Síntomas de Inseguridad**:**

La seguridad lógica y la seguridad física dan mucho que desear, ya sea por falta de actualización de recursos o software. La continuidad del servicio empieza a fallar es decir el tiempo de respuesta para una petición es demasiado largo. Bajo estas circunstancias es notorio que la empresa necesita pasar por una auditoria de seguridad informática. (Flores, 2010)

3.6.5 Herramientas y técnicas para la auditoria informática

Las herramientas para una auditoria informática se basan en cuestionarios, entrevistas, checklist, Trazas y/o Huellas y Normas encargadas en la gestión de la seguridad de la información. Entrevistas.- el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas, en ellas recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos.

Checklist.- son preguntas leídas o recitadas de memoria donde el auditor consigue obtener respuestas coherentes que permitan una correcta descripción de los puntos débiles y fuertes de determinado sistema o recurso informático.

Trazas y/o Huellas.- Son programas informáticos que se encarga de rastrear el camino de los datos a través de la red y su buen funcionamiento, estos software no deben alterar el buen funcionamiento de los sistemas, si esto sucediera se convendrá de antemano las fechas y horas más adecuadas para su empleo (Lizcano, 2011)

3.6.6 Metodología de trabajo de auditoría de seguridad informática

El método de trabajo del auditor pasa por las siguientes etapas, según Astudillo (2011):

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

3.6.6.1 Alcance de la auditoría de seguridad

El alcance de la auditoría es asesorar a la gerencia o al departamento informático de la empresa de la existencia de fallas y errores para que la gerencia delegue las funciones respectivas, manteniendo un adecuado control sobre la organización, de esta manera se reduce los niveles mínimos el riesgo inherente, y se consigue mayor eficiencia y eficacia en la empresa. En esta sección se deja claro de cuáles son los límites a auditar, debe existir ese acuerdo entre auditores y clientes. Los auditores

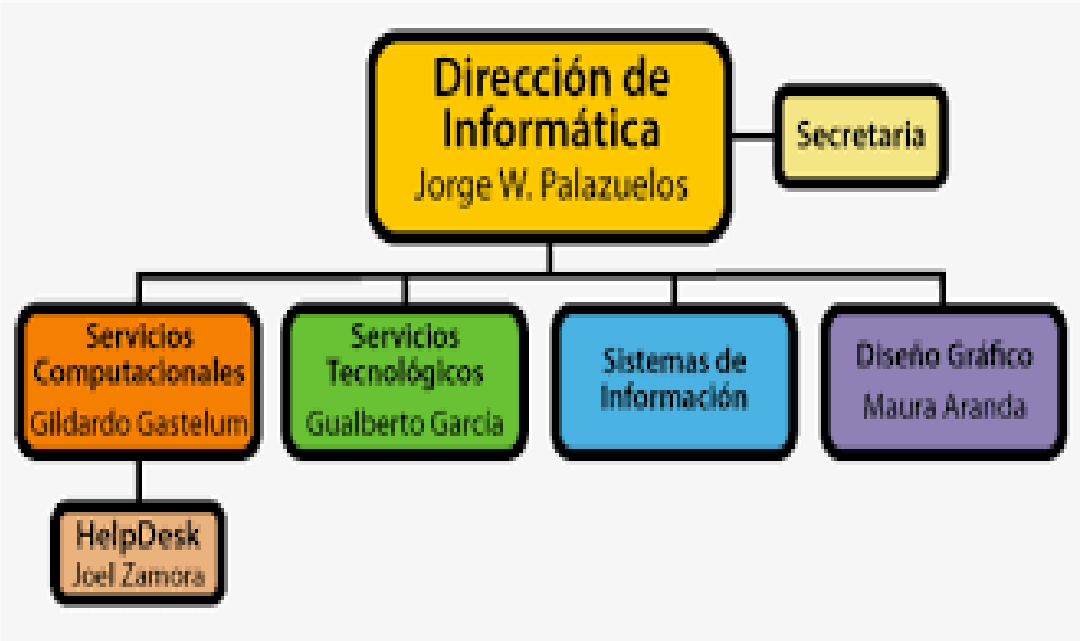
deben conocer con la mayor precisión los objetivos a los que su tarea debe llegar. Han de comprender los deseos y pretensiones del cliente, de forma que las metas establecidas puedan ser consumadas.

3.6.6.2 Estudio Inicial

Se inicia examinando las actividades y funciones generales de la empresa. El auditor debe conocer lo siguiente para su realización.

- **Organigrama:**

El organigrama expresa la estructura oficial de la organización a auditar (Aldaz, 2011)



- **Departamentos:**

El equipo auditor describirá brevemente las funciones de cada uno de los departamentos. Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. (Aldaz, 2011).

- **Flujos de Información:**

El flujo de información entre los diferentes departamentos son necesarios para su eficiente gestión, La información en circulación no debe no distorsionar la estructura de la organización (Aldaz, 2011).

Es muy frecuente que en las organizaciones se creen canales alternativos de información, que ayudan a los departamentos a ejercer sus funciones; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa. Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización

- **Número de Puestos de trabajo**

Los Puestos de Trabajo de la organización deberán corresponder a las funciones para las que están designadas. Es habitual que bajo nombres diferentes se realicen funciones iguales, esto exterioriza que hay funciones operativas redundantes (Aldaz, 2011)

- **Número de personas por Puesto de Trabajo**

La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

3.6.6.3 Entorno Operacional

Aldaz (2011) menciona que: El equipo auditor debe conocer el entorno donde va a realizar sus funciones para esto es necesario estar al tanto de lo siguiente:

Situación geográfica de los sistemas.- se determina la ubicación de los distintos sistemas o centros de procesos de datos en la empresa y se verifica los responsables de cada uno de ellos.

Arquitectura y configuración de Hardware y Software.- Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

Inventario de Hardware y Software.- El equipo auditor deberá recabar información escrita, a manera de inventario donde consten todos los elementos físicos y lógicos de la instalación. En cuanto a los elementos físicos están las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc. En los elementos lógicos constan, el software básico es decir los sistemas operativos de las PCs, los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables

Comunicación y Redes de Comunicación.- En esta primera etapa los auditores dispondrán del número, situación y características principales de las líneas de comunicación, así como de la acometida de la línea de internet a las instalaciones de la empresa, También se tendrán la información de las subredes Locales de la Empresa.

3.6.6.4 Determinación de recursos de la auditoría Informática

Refiriéndose a los recursos de la auditoría Aldaz (2011) expresa que: Una vez analizados el entorno operacional y detallado el estudio inicial se procede a determinar los recursos que han de emplearse en la auditoria.

3.6.6.4.1 Recursos materiales

Los recursos materiales del auditor son softwares muy potentes y flexibles que permiten al auditor evaluar los sistemas informáticos con el único fin de detectar anomalías, también las computadoras, que se las puede denominar tiempo de máquina o espacio de disco, las impresora; estos recursos son parte de la empresa y que son prestadas por un determinado tiempo para realizar las labores propias de un auditor.

3.6.6.4.2 Recursos Humano

Los recursos humanos depende del tamaño de la empresa hacer auditada, generalmente el equipo auditor son profesionales con una larga experiencia en el campo informático entre ellos están las personas: experto en desarrollo de proyectos, técnico de sistemas, experto en bases de datos y administración de las mismas, experto en software de comunicación.

3.6.6.5 Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a. Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b. Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

3.6.6.6 Informe Final

En el informe final se exteriorizan las debilidades encontradas con sus respectivas sugerencias que se debieran implementarse ante la ausencia o la falla en los controles para el tratamiento de la seguridad de la información. Estas recomendaciones están avaladas por las normativas que el auditor desee basarse.

3.6.6.7 Estructura del informe final

En el informe solo se debe detallar los hechos importantes, los hechos poco significativos desvía la atención del lector, por lo tanto el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Inmediatamente se define los objetivos y el alcance de la auditoría (Rojas, 2011)

Enumeración de temas considerados:

Se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría, y para cada tema, se seguirá el siguiente orden a saber:

a. Puntos débiles y amenazas. Se refiere a las falencias encontradas en cada elemento evaluado.

b. Efectos. Trata de las posibles acciones que se pudieran presentar si no se toma medidas de protección en los puntos débiles.

c. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática. Aquí se expone las diferentes sugerencias necesarias para contrarrestar las debilidades. (Gonzáles, 2013)

3.7 Estándares relacionados con la seguridad informática

Actualmente existen varios estándares certificables que garantizan la protección de los Sistemas Informáticos así como un buen uso de la información. Poseer alguno de estos estándares significa que la tecnología de la información va a tener cierto grado de protección adicional.

El principal estándar de seguridad informática y de la información, que define los requisitos de auditoría y sistemas de gestión de seguridad de la información es el ISO/IEC 27001[13]. Este estándar puede usarse en conjunción con el ISO/IEC 27002[14],

[13] Sistemas de Gestión de la Seguridad de la Información
[14] Código de Prácticas para la gestión de la Seguridad de la Información.

desarrollado a partir de la norma BS7799[15], publicado a mediados de la década de 1990. La norma británica fue adoptado por la ISO/IEC como ISO/IEC 17799:2000[16], revisada en 2005, el cual se conforma como un código internacional de buenas prácticas de seguridad informática y de la información. (Economía, sf) Existen otros estándares de carácter más general que también cubren la seguridad informática como parte del desarrollo de una infraestructura de tecnología de la información completa. Ejemplos de este tipo son COBIT[17], ITIL[18], OSSTMM[19]. Estos estándares surgen como buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información. (Tony, 2011)

3.7.1 NORMA NTP-ISO/IEC 17799:2007

3.7.1.1 Reseña histórica

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. (Norma 17799, 2011)
La seguridad de la información se define como la preservación de:

- Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

[15] Es un estándar Británico de Gestión de seguridad publicada en mayo de 1999
[16] Técnicas de Seguridad para la Tecnología de la Información.
[17] Objetivos de Control de la Tecnologías de la Información
[18] Biblioteca de Infraestructura de Tecnologías de Información
[19] El Manual de la Metodología Abierta de Comprobación de la Seguridad

- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. En 1995 el British Standard Institute publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información, en 1998, también el BSI publicó la norma BS7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002; tras una revisión de ambas partes de BS7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Aplicable por toda organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la tecnología.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (Villalón, 2010)

3.7.1.2 Definición de la norma NTP-ISO/IEC 17799:2007

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), mediante el Sistema 1 u Adopción, durante los meses de junio a julio del 2006, utilizando como antecedente a la Norma ISO/IEC 17799:2005 Information technology – Code of practice for information security management. El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) presentó a la Comisión de Reglamentos Técnico y Comerciales -CRT-, con fecha 2006-07-21, el PNTP-ISO/IEC 17799:2006 para su revisión y aprobación; siendo sometido a la etapa de Discusión

Pública el 2006-11-25. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2ª Edición, el 22 de enero del 2007 (NTP-ISO/IEC 17799, 2007)

3.7.1.3 Estructura y campo de aplicación

Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo. Las clausulas son las siguientes:

- Política de seguridad;
- Organizando la seguridad de información;
- Gestión de activos;
- Seguridad en recursos humanos;
- Seguridad física y ambiental;
- Gestión de comunicaciones y operaciones;
- Control de acceso;
- Adquisición, desarrollo y mantenimiento de sistemas de información;
- Gestión de incidentes de los sistemas de información;
- Gestión de la continuidad del negocio;
- Cumplimiento;

Dentro de cada clausula, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una

guía para su implantación. Para este proyecto se considera previamente cuantos son realmente los aplicables según las necesidades (Norma Técnica Peruana NTP-ISO/IEC 17799, 2007)

3.7.1.3.1 Política de seguridad

Es un documento que manifieste por escrito cómo una empresa planea proteger la tecnología de la información de la compañía (IT). Una política de seguridad es a menudo considerada como un documento vivo, lo que significa que el documento no está terminado, ya que se actualiza continuamente basado en los requerimientos de la empresa. (NTP-ISO/IEC 17799, 2007)

Este documento es comunicado a los empleados en forma adecuada y entendible para su cumplimiento, se debe tener cuidado de no distribuir fuera de la empresa con el fin de no compartir información confidencial.

3.7.1.3.2 Organizando la seguridad de información

La organización de la información se lleva a cabo mediante la asignación de funciones encaminadas a la gestión de la información, a ciertos empleados de la empresa, estas responsabilidades deben ser tomadas con la seriedad del caso y ser definidas claramente. Los requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente. (NTP-ISO/IEC 17799, 2007)

3.7.1.3.3 Gestión de activos

Para la gestión de activos es necesario tener un inventario de los activos, y asignarlos a cada uno un propietario que se encargue de su buen funcionamiento y

operación del mismo. Como es lógico han de existir diferentes tipos de activos, unos más importantes que otros, dependiendo de la información que posean, por esta razón unos se les brindará más protección que otros. (NTP-ISO/IEC 17799, 2007)

3.7.3.3.4 Seguridad en recursos humanos

Tiene como fin asegurar que los empleados, contratistas y terceras personas comprendan sus responsabilidades en el uso de los recursos de la empresa con el único objetivo de reducir el riesgo de robo, fraude o mal uso de las instalaciones. Este tipo de funciones deben ser documentadas en afinidad con la política de la empresa, de tal manera que los empleados contratistas y terceros, puedan recibir el entrenamiento adecuado de las responsabilidades de sus funciones. (NTP-ISO/IEC 17799, 2007)

3.7.1.3.5 Seguridad física y ambiental

Su objetivo es restringir el acceso físico a los recursos informáticos para ello deben haber controles adecuados en las entradas a áreas donde exista equipos con información sensible, de tal manera que se de ingreso solo a personas autorizadas. Otro punto que se debe tomar en cuenta es el riesgo de amenazas del entorno como fallos de energía, fallo de la línea de datos externa, inundaciones, terremotos; para los cuales se debe designar y aplicar protección física (NTP-ISO/IEC 17799, 2007).

3.7.1.3.6 Gestión de comunicaciones y operaciones

Su objetivo es de garantizar la operación correcta de la información para ello se ha de establecer procedimientos operativos adecuados para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado. También deben ser consideradas la

integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad (NTP-ISO/IEC 17799, 2007).

3.7.1.3.7 Control de acceso

Su objetivo es controlar el acceso a la información, con la elaboración de una política de control basada en los requerimientos de seguridad de la organización, un ejemplo claro es el control de la asignación de contraseñas para dar un acceso a los recursos informáticos solo a personas previamente capacitadas en el tema (NTP-ISO/IEC 17799, 2007).

3.7.1.3.8 Adquisición, desarrollo y mantenimiento de sistemas de información

Su objetivo es de afirmar que la seguridad esté imbuida dentro de los sistemas de información. Se refiere concretamente al software empleado para almacenar información, ya sea este adquirido o desarrollado por los empleados, es decir incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios (NTP-ISO/IEC 17799, 2007).

3.7.1.3.9 Gestión de incidentes de los sistemas de información

Su objetivo es que la gerencia tenga medidas de contingencias oportunas para dar una respuesta rápida y eficiente ante los reportes de debilidades en la seguridad de la información, estos tipos de eventos deben ser reportados lo más rápido posible a través de una gestión de canales apropiados, para ello todo usuario debe informar acerca de la debilidad de los sistemas y servicios de información (NTP-ISO/IEC 17799, 2007).

3.7.1.3.10 Gestión de la continuidad del negocio

Su objetivo es desarrollar planes de mantenimiento y recuperación ante grandes fallos o desastres de los sistemas de información, que garanticen la continuidad del negocio, los eventos que pueden interrumpir la operación normal de la empresa han de ser identificados, junto con la probabilidad e impacto de dichas complicaciones y sus consecuencias para la seguridad de información (NTP-ISO/IEC 17799, 2007).

3.7.1.3.11 Cumplimiento

Su objetivo es de evitar incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad, se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información (NTP-ISO/IEC 17799, 2007).

4 METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD (OSSTMM ISECOM)

4.1 Introducción

Como su nombre lo dice es un manual que describe una metodología aplicable a las pruebas de la seguridad, para fines prácticos solo se describen los puntos de mayor importancia y se presentan de manera esquemática para dar al lector un panorama general de los procesos en el análisis y pruebas de la seguridad.

El OSSTMM debe cumplir con las reglas establecidas en las diferentes Leyes tanto Internacionales, Federales, Locales, Industriales y Políticas establecidas en la organización.

Cada una de las acciones debe prever no violar alguna ley, reglamento o política y cada una de las actividades deben ser coordinadas con la organización que requiere la implementación de este tipo de pruebas a su seguridad.

Contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras.

4.2 Tipo de Test

Las pruebas de seguridad pueden abarcar todas las formas y tipos como la intrusión hasta la auditoría guiada.

En el OSSTMM contempla 6 tipos de Test.

4.2.1 Blindado

El auditor establece el objetivo sin el conocimiento de su defensa, activos o canales. El objetivo es preparado para la auditoría conociendo todos los detalles de la misma. En este tipo es lo que se conoce también como “Hacking Ético”.

4.2.2 Doble Blindaje o “Double Blind”

El objetivo no es notificado con anticipación de los alcances de la auditoría, canales de prueba o prueba de vectores. Este también se conoce como Auditoría de Caja Negra o Pruebas de Penetración.

4.2.3 De Caja Gris

El Auditor establece el objetivo con un conocimiento limitado de su defensa, activos y todos los canales conocidos. El objetivo es preparado para la auditoría conociendo el avance y detalles de la misma.

4.2.4 Doble Caja Gris

El auditor establece el objetivo con conocimiento limitado de la defensa, activos y sus canales. El objetivo es notificado del ámbito y tiempo de cada marco de la auditoría pero no de los canales puestos a prueba ni de los vectores.

4.2.5 Tándem o Secuencial (Tandem)

El auditor y el objetivo están preparados para la auditoría y ambos conocen los avances y detalles de la auditoría. Se establece una serie de pruebas de protección

(Tandem test) y controles del objetivo. Es una prueba minuciosa de acuerdo al visión del auditor del total del análisis. Este es un proceso transparente por lo que se le llama de Caja de Cristal en el cual tanto el auditor como el objetivo trabajan en las pruebas.

4.2.6 Inverso

El auditor participa con el objetivo de manera completa en el proceso de la seguridad operacional. Pero el objetivo no conoce el ¿Qué?, ¿Cómo? Y ¿Cuándo? el auditor realizará las pruebas. La meta es desconocida en este tipo de pruebas. La amplitud y profundidad depende de la calidad de la información provista al auditor. Esto permite por lo regular lo que se llama un Ejercicio de Equipo Rojo (Read Team Exercise).

4.3 *Ámbito o competencia*

El ámbito debe abarcar toda la seguridad operativa y comprometerse en las diferentes áreas o canales como lo describe el manual: Seguridad en las comunicaciones, Seguridad Física y Seguridad del Espectro electromagnético, como se muestra en la Tabla 4.3.1

Canal	Sección	Descripción
Seguridad Física	Humano	Todo el elemento humano comprometido en la organización
	Físico	Todo lo referente a instalaciones y cualquier objeto tangible en la organización.
Seguridad de las Comunicaciones	Redes de datos	Incluye todos los sistemas electrónicos y redes de datos que interactúan en la organización

	Telecomunicaciones	Son todas las comunicaciones digitales o analógicas empleadas para la comunicación entre redes
Seguridad del espectro electromagnético	Comunicaciones Inalámbricas	Se incluyen todas las señales electromagnéticas empleadas tanto en las comunicaciones como cualquier otra emanación del espectro.

Tabla 4. 3.1.: Ámbito o competencia de la seguridad.

4.4 *Módulos*

El flujo del manual OSSTMM comienza con situación del objetivo. La situación está dada por la cultura, reglas, normas, regulaciones, legislación y políticas definidas en el objetivo. Y al final se obtiene una comparación de todas las alarmas, alertas, reportes o registros de accesos.

Esta metodología propone un modelo jerárquico de “CANALES, MÓDULOS Y TAREAS”

Los Módulos son áreas específicas de cada canal, pudiendo encontrar actividades que se encuentren en la frontera entre dos canales, por ejemplo una red inalámbrica puede ser analizada como una Red de datos y al mismo tiempo en el ámbito del análisis del espectro electromagnético.

En general esta metodología propone dividir el trabajo de la auditoría clasificándolos por canales, módulos y tareas. Los vectores son simplemente las líneas de análisis que apuntan a cada uno de los canales.

4.5 Pruebas de seguridad en la red de datos

Las pruebas de seguridad en la red requieren de la interacción entre la red de datos y el control de acceso del propietario.

Para determinar la calidad de las pruebas se deben tener las siguientes consideraciones:

4.5.1 Ignorancia o conocimiento de la legislación involucrada

Se deben tomar en cuenta todas las leyes involucradas tanto nacionales, regionales y políticas internas de la organización.

4.5.2 Derechos de propiedad

Solo se realizarán pruebas en sistemas que estén dentro del ámbito de competencia del analista de la seguridad, evitando invadir o violar la propiedad de los involucrados.

4.5.3 Calidad

Se debe procurar la calidad por encima de la cantidad, debiendo evitar realizar una cantidad pruebas que no se realicen a detalle, no por analizar más canales o módulos se descuiden aspectos importantes o críticos de la seguridad.

4.6 *Esquema general*

Antes de describir cada fase y sus actividades se muestra el esquema general para una mayor comprensión del proceso de las pruebas de la seguridad como se muestra en la figura 4.5.1.

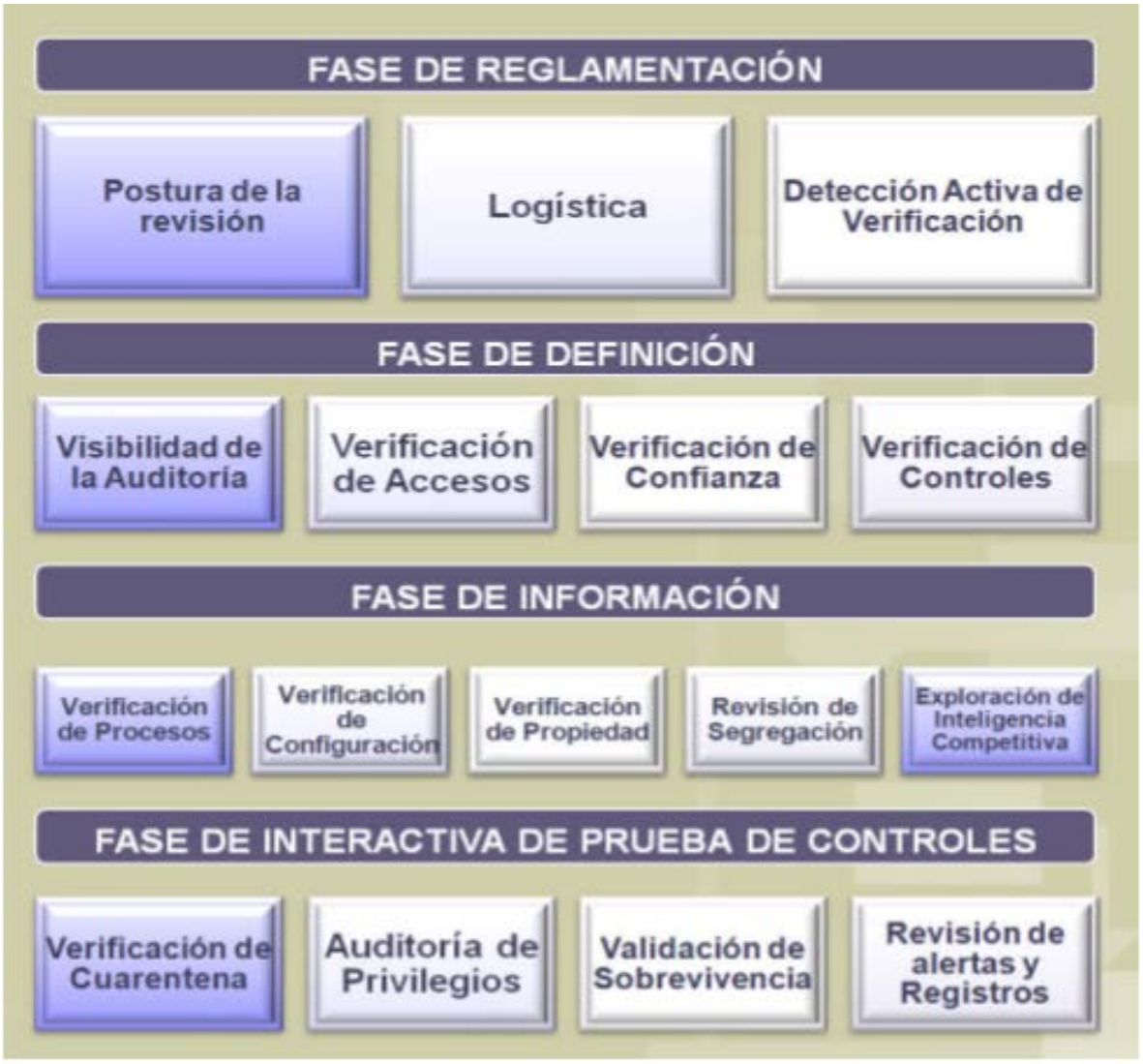


Figura 4-1.

Esquema General de las Pruebas de Seguridad

4.7 *Fase de reglamentación*

Es la fase en la que se establece la dirección de las pruebas, el auditor comienza con la comprensión de la auditoría, los requisitos, el alcance y las limitaciones.

4.7.1 Postura de la revisión

El estudio inicial de la postura de las pruebas debe considerar las leyes, ética, políticas, regulaciones industriales y cultura con respecto a la seguridad.

- Política: Revisar y documentar todos los requerimientos de la política de seguridad, integridad y privacidad dentro de su ámbito.
- Legislación y regulación: Revisar y documentar la legislación regional, nacional y cualquier otra regulación industrial que resguarde la seguridad y privacidad de acuerdo a los requerimientos de la organización.
- Cultura: Revisar y documentar la cultura organizacional.
- Era o época: en lo que se refiere a la edad y generación de los sistemas, software y la aplicación de los servicios que se requieren para la operación.
- Partes débiles: Revisar y documentar cualquier sistema, software y aplicación de servicios que puedan causar alguna inestabilidad dentro de la organización.

4.7.2 Logística

Esta es la preparación de los canales para el desarrollo de la evaluación necesarios para la prevención de falsos positivos y falsos negativos que nos puedan llevar a resultados inexactos.

- Estructura
- Calidad de la red de datos
- Tiempo

4.7.3 Detección activa de verificación

Determinar los controles activos y pasivos de detección de intrusos para filtrar y denegar intentos de las pruebas con anterioridad para reducir los riesgos de corromper los datos de los resultados de las pruebas.

4.8 Fase de Definición

En esta fase se define el ámbito de la aplicación. La base de las pruebas de seguridad requiere el conocer el ámbito y el alcance en relación con las interacciones de los objetivos transmitidos con los activos

4.8.1 Visibilidad de la auditoría

Se enumeran los objetivos (blancos de pruebas) en el ámbito que interactúan directa o indirectamente entre los sistemas.

En este punto se observan aspectos como identificación y delimitación del segmento de red, verificar respuestas icmp, es decir, se describen puntos específicos de evaluación, donde se verifica cada servicio, puerto y aplicación de la red.

4.8.2 Verificación de accesos

En este punto se deben enumerar todos los puntos de acceso a la red de datos tomando en cuenta el entorno. Se deben revisar 3 aspectos importantes: Los procesos de acceso, Servicios y Autenticación.

4.8.3 Verificación de confianza

Se realizan pruebas para comprobar la confianza entre los sistemas buscando un entorno seguro en lo que se refiere al acceso a la información o la propiedad física para lo cual se necesita la identificación y la autenticación.

Para ellos se realizan pruebas de “Spoofing, Phising y de abuso de recursos”

- Spoofing o Suplantación: Se realizan pruebas de suplantación en la red, probando

- “Phishing” es una técnica para realizar fraudes electrónicos donde se envía una liga a una página web, donde al acceso o descarga de algún archivo se incluye código malicioso para obtener información o accesos no autorizados. El objetivo es comprobar las direcciones URL de las peticiones o mensajes.

- Abuso de recursos: Probar la profundidad de los accesos a la información y servidores sin necesidad de credenciales o identificación en la organización. Verificar la continuidad de las métricas especialmente el balanceo de cargas para prevenir que usuarios abusen de los recursos

4.8.4 Verificación de controles

Verificar y enumerar la funcionalidad operacional que asegure la disponibilidad de los activos y los servicios. Para este punto se deben realizar las siguientes pruebas:

- No repudio: Enumerar y probar los sistemas con pruebas de acceso, verificar los registros de accesos, las interacciones con el propietario y buscar cualquier evidencia de repudio o negación del acceso.

- Confidencialidad: Enumerar todas las interacciones de los servicios con su entorno dentro de las comunicaciones verificando líneas seguras por medio del cifrado. Y verificar los métodos de confidencialidad utilizados en las comunicaciones fuera de los límites.

- Privacidad: Enumerar los servicios en el ámbito de las comunicaciones o activos transportados específicos, mediante firmas, identificación personal y todas las interacciones con el fin de proteger la propiedad y los servicios, proporcionando estos, solo a quienes deban ser compartidos o entregados.

- Integridad: Enumerar las deficiencias y poner a prueba la integridad de los activos y servicios, comprobando que estos no puedan ser modificados o alterados sin autorización y conocimiento del propietario.

4.9 Fase de Información

En esta fase el auditor va descubriendo información, aquí se expone la mala gestión de la información.

4.9.1 Verificación de procesos

En esta etapa se deben realizar pruebas para examinar el mantenimiento de la seguridad funcional en el establecimiento de procesos como se define en la Postura de la Revisión.

- Mantenimiento: Examinar y documentar las líneas de tiempo, oportunidades, accesos y alcance de los procesos para la notificación y respuesta de seguridad de la red y el monitoreo de la seguridad.

- Desinformación: Determinar la medida en que las notificaciones de seguridad y alarmas pueden ampliarse o alterarse con información errónea.

- Proceso diligente conveniente: Mapear y verificar cualquier laguna entre la práctica y los requerimientos determinados en la Postura de Revisión a través de todos os canales.

- Identificación: Documentar y enumerar los objetivos o blancos y los servicios en los que se puede cometer algún abuso.

4.9.2 Verificación de Configuración

Se deben revisar todas las configuraciones implementadas en los controles de acceso, aplicaciones y dispositivos.

- Controles de Configuración: Examinar los controles para verificar la configuración de referencia de los Sistemas Operativos, aplicaciones y equipamiento para validar configuraciones seguras. Y examinar las Listas de Control de Acceso (ACLs).

- Errores comunes en las Configuraciones: Verificar los servicios disponibles que no son necesarios o redundantes, verificar las configuraciones por default y verificar la administración ya sea local o remota.

- Mapeo Sensible: Mapear las limitaciones de seguridad descubriendo la áreas sensibles, realizar el análisis de procedimientos actuales, manejo de información confidencial y sensible y la relación con las políticas de seguridad.

- Sensibilidad al “Hijacking”: El “hijacking” es un término empleado en aspectos de seguridad informática que se aplica para el robo, o por decirlo de otra forma, secuestro de información, sesión o algún activo. Para este punto se debe descubrir

y examinar la medida en que personas no oficiales que puedan proporcionar información errónea con el fin de obtener información o acceso no autorizado.

4.9.3 Validación de Propiedad

Probar y examinar información y datos disponibles que sirvan para obtener una autenticación ilegal.

- Compartir Recursos: Verificar el grado en que un recurso o licencia individual, privada, que no se reproduce, no libre o no abierta es compartida ya sea intencionalmente o mediante el intercambio de procesos, programas, bibliotecas o involuntariamente mediante una mala gestión de licencias o recursos.

- Mercado Negro: Verificar el grado en que un recurso o licencia se promueve o comercializa ilegalmente por personal o por la organización.

- Canales de venta: Comprobar si alguien fuera del ámbito de la organización vende activos propiedad de la organización.

4.9.4 Revisión de Segregación

Realizar pruebas para verificar la separación de la información personal privada y la de la organización.

Se requiere ubicar las localidades más importantes de información privada.

4.9.5 Verificación de Exposición

Se deben realizar pruebas para descubrir información que proporcione acceso un área y que permita múltiples accesos a otras áreas.

4.9.6 Exploración de la Inteligencia Competitiva

Realizar pruebas de barrido de información que pueda ser analizada como inteligencia de negocio. Esto puede ser con fines de espionaje industrial.

No se limita a las relaciones comerciales, también incluye empleados, socios, distribuidores, contactos, finanzas, estrategias y planes.

4.10 *Fase Interactiva de pruebas de controles*

Estas pruebas se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de la seguridad y esta fase no puede ser realizada hasta que las otras fases se hayan terminado.

Es probable que sea necesario revisar y repetir pruebas que no arrojaron resultados para confirmar los datos.

4.10.1 Verificación de cuarentena

Probar y verificar las áreas de contención de elementos agresivos y hostiles para la organización. Se deben tomar en cuenta dos puntos:

- Identificación y contención de procesos: Identificar y examinar los métodos de cuarentena para contener elementos hostiles como agentes de ventas, caza recompensas, personal de paso por la organización, personal de la competencia y cualquier elemento que pueda obtener algún beneficio de la información. Esto aplica a procesos automatizados en la red de datos.

- Niveles de contención: Verificar el estado de contención y el tiempo de contención.

4.10.2 Auditaría de Privilegios

Se deben realizar pruebas a las credenciales de usuarios y los permisos con los que cuentan.
Para ello se debe examinar la identificación, autorización y el escalamiento.

4.10.3 Validación de Sobrevivencia

Determinar y medir la resistencia de los objetivos auditados a los cambios excesivos u hostiles a los que puedan estar propensos.

La denegación de servicio es una situación donde una circunstancia, intencional o accidentalmente, impide que el sistema funcione correctamente, y es común que un sistema funcione incorrectamente en ciertas condiciones como el aumento de carga o el cambio de algunos parámetros.

Para ello se debe verificar tres aspectos:

- Resistencia: Detectar los puntos individuales de fallo, verificar el impacto y las consecuencias en la operación.

- Continuidad: Enumerar y probar los tiempos de respuesta para que se restaure el sistema.

- Seguridad: Mapear y documentar los procesos de apagado de los sistemas en caso de emergencia.

4.10.4 Revisión de Alertas y Registros

Realizar un análisis de las deficiencias entre las actividades realizadas con las pruebas y la verdadera profundidad de las actividades registradas.

- Alarmas: Verificar y enumerar el uso de un localizador de eventos, registros, avisos de peligro o mensajes de accesos donde se conozca o sospeche de ataques, ataque por ingeniería social, intentos o cualquier actividad fraudulenta.

- Almacenamiento y recuperación: Se debe documentar y verificar los accesos no privilegiados a las alarmas, registros y notificaciones a los sitios de almacenamiento.

4.11 Ventajas.

- **Ventajas OSSTMM**

  - Cuenta con manuales fáciles de entender y aplicar.
  - No se necesita de una persona especialista para realizar la auditoria.
  - Su metodología se encuentra disponible en diversos Idioma.
  - Existe versiones gratuitas y pagas. La versión paga es de bajo costo.
  - Las versiones más antigua se pueden descargar en forma gratuita

- **Auditorias en diversos niveles:**

    - Páginas Web.
    - Sistemas informáticos
    - Red.
    - Procedimiento.

- **Costos y beneficios.**

    - Metodología prácticamente gratuita. Y no se necesita un especialista.

5 COBIT: MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios. Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se

auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

"La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

5.1 Planificación y organización

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

5.1.1 Adquisición e implantación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

5.1.2 Soporte y servicios

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

5.1.3 Monitoreo

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

5.2 Usuarios

- La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

- Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

- Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

- Los Responsables de TI: para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

5.3 Características

- Orientado al negocio

- Alineado con estándares y regulaciones "de facto"

- Basado en una revisión crítica y analítica de las tareas y actividades en TI

- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI. Requerimientos de la información del negocio: Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios: Requerimientos de Calidad: Calidad, Costo y Entrega. Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

5.3.1 Efectividad

La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

5.3.2 Confiabilidad

Proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.

5.3.3 Eficiencia

Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).

5.3.4 Cumplimiento

Cumplimiento de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad

5.3.5 Disponibilidad

Accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma. En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

5.3.6 Datos

Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.

5.3.7 Aplicaciones

Entendidas como sistemas de información, que integran procedimientos manuales y sistematizados.

5.3.8 Tecnología

Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

5.3.9 Instalaciones

Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

5.3.10 Recursos humanos

Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información, o de procesos de TI.

5.4 Tecnologías de información

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información

- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información

- El costo de las inversiones actuales y futuras en información y en tecnología de información; y

- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la respalda, representan los activos más valiosos de la empresa, por lo que la gestión de los riesgos asociados de la Tecnología de Información, o Gobernabilidad de TI (IT Governance), ha ganado notoriedad en tiempos recientes como un aspecto clave de la gobernabilidad corporativa, dada su capacidad de proporcionar valor agregado al negocio, balanceando la relación entre el riesgo y el retorno de la inversión sobre TI y sus procesos. Estos aspectos se enfatizan en el Marco de referencia COBIT, el cual se define como conjunto de Objetivos de Control para la Información y Tecnologías Relacionadas.

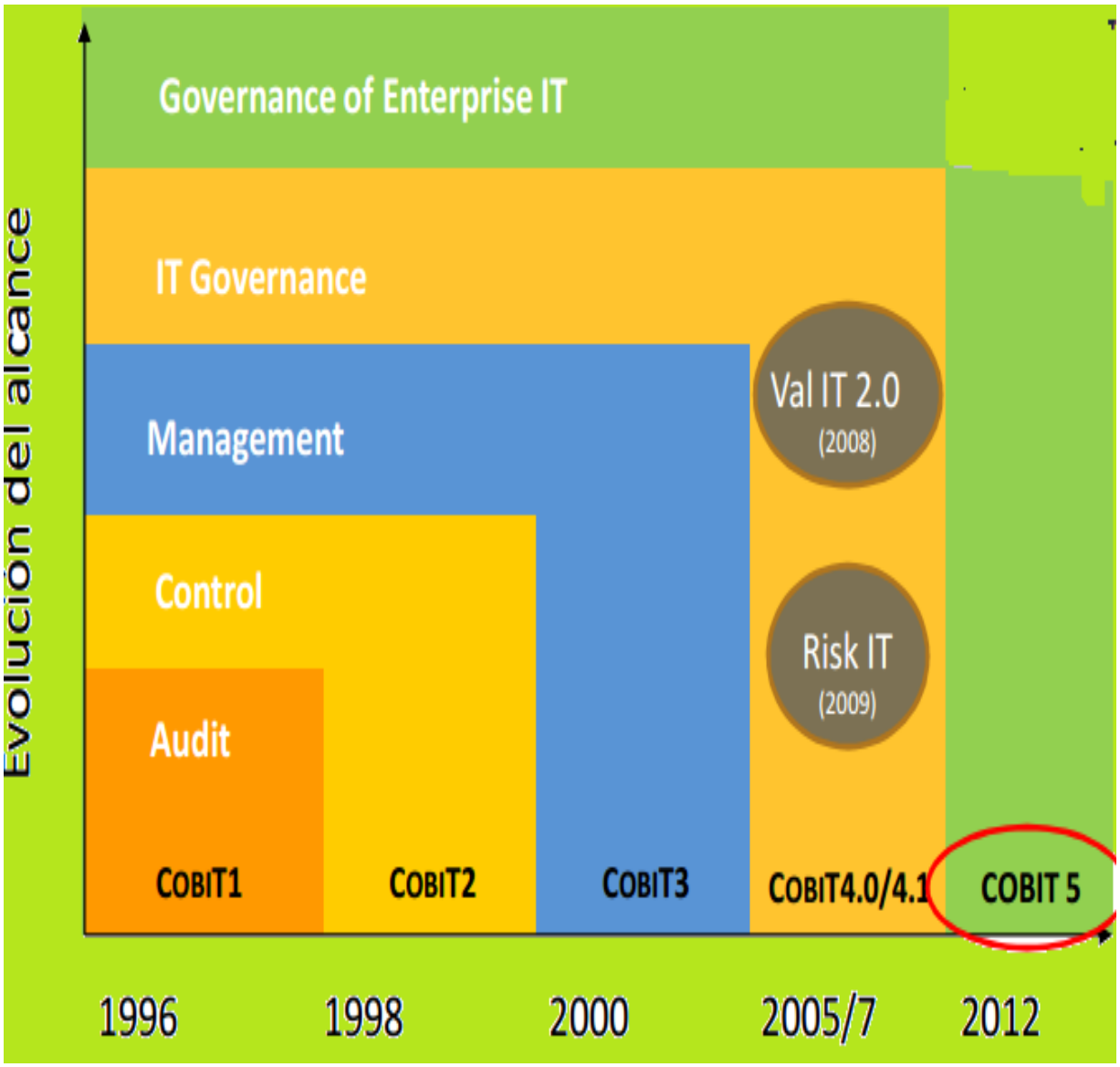
Bajo este escenario, una adecuada administración de los recursos de TI es fundamental para mejorar la calidad de los productos y servicios brindados por el área, lo que se reflejará en mejoras en los procesos que respalda, y en el nivel de seguridad y control con el cual se trabaja, elevando su capacidad para satisfacer los objetivos de cumplimiento definidos en la estructura de control interno de la organización, reduciendo además los costos administrativos asociados al entorno informático.

(COBIT), define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro (4) “dominios” principales, a saber:

- Planificación y organización
- Adquisición e implantación
- Soporte y Servicios
- Monitoreo

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. En conjunto, estos dominios y los objetivos de control, facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporciona la Tecnología de Información, tales como: datos, sistemas de aplicación, tecnología (plataformas), instalaciones y el recurso humano.

5.5 Evolución de COBIT 5.0



5.5.1 Gobierno TI

Se entiende por Gobierno TI (“IT Governance”), el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. Constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que TI soporta y facilita el desarrollo de los objetivos estratégicos definidos.

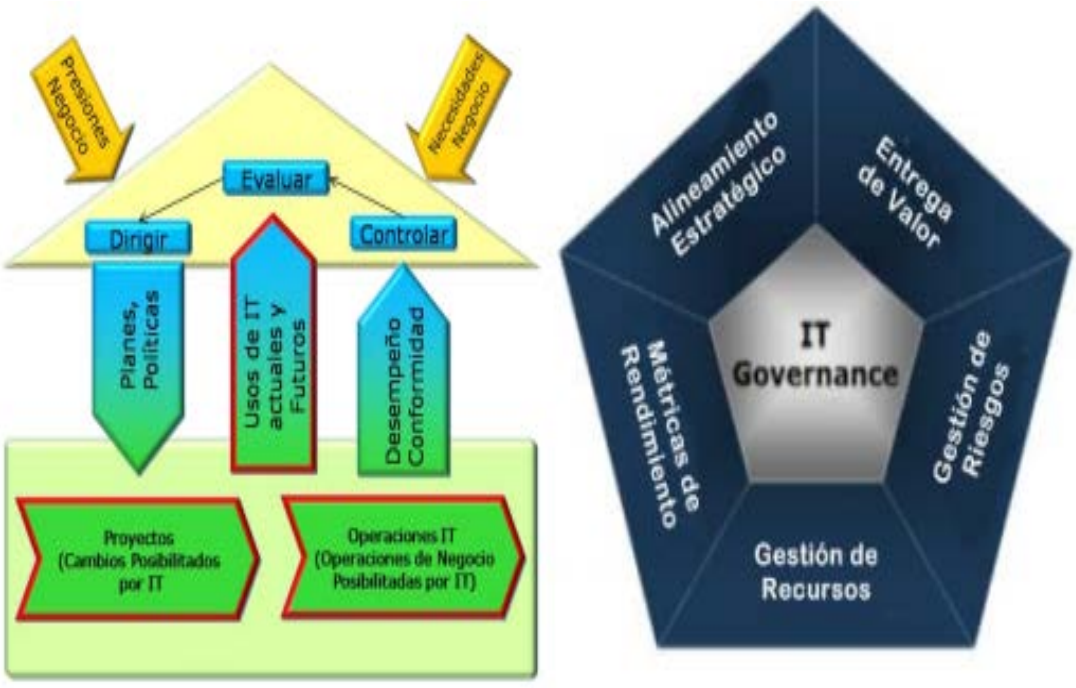
Se necesita de un marco de referencia base para su implementación que esté dirigido por el control de métricas. El negocio necesita conocer el estado de sus recursos y procesos TI, cómo aportan valor y cómo evolucionan, para ello existen varias alternativas tales como la ISO 38500, Cobit, ITIL, CMMI, Project Governance, Risk Management, etc. Por lo tanto podríamos decir que el Gobierno de TI, se compone de la supervisión, estructuras y procesos organizacionales que garanticen que la organización de TI sustente las estrategias y objetivos de toda la empresa, a través de los siguientes logros:

- TI está alineada con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros.
- Integración e institucionalización de las buenas prácticas
- Satisfacer los requerimientos de calidad, fiduiciarios y de seguridad
- Optimizar recursos y balancear riesgos y oportunidades

En realidad muy pocos ejecutivos pueden describir lo que significa “IT Governance” y en la práctica, en la mayoría de los casos no lo han diseñado o lo desarrollaron solo para el cumplimiento de problemas específicos. La norma ISO 38500 aporta claridad al

tema de la Gobernabilidad de TI y proporciona un marco basado en seis principios rectores de un buen gobierno corporativo de TI (Responsabilidad, Estrategia, Adquisición, Rendimiento, Conformidad, Comportamiento) y un modelo para gobernar las TI con tres tareas principales: evaluar, dirigir y controlar.

El gobierno de TI se agrupa en cinco áreas: Alineamiento estratégico (vinculando TI con los planes de negocio), Entrega de valor (ejecutando la propuesta de valor ofrecida), Gestión de Riesgos (aversión o propensión al riesgo), Gestión de Recursos (supervisión e inversiones), Mediciones de Performance (seguimiento y control).



5.5.2 Desarrollo COBIT 5

Una sólida plataforma subyacente a la norma ISO 38500 es COBIT, que es una buena referencia para las políticas, los procesos, las estructuras y los controles necesarios para implementar el sistema de gestión que ayuden a la gobernabilidad. Con Cobit se puede lograr la alineación de TI al negocio y utilizarlo como punto de partida para la adaptación de los procedimientos específicos. ISACA publicó el año pasado una nueva versión del ya conocido estándar Cobit para el cumplimiento de objetivos de control para el CIO y su área. Esta versión, profundamente revisada y mejorada, provee un marco de referencia integral que contribuye en la organización al logro de los objetivos y entrega de valor a través de un efectivo gobierno y gestión de la TI empresarial.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

El marco COBIT 5 se construye sobre cinco principios básicos, y 7 catalizadores o habilitadores para el gobierno y la gestión de TI de la empresa.

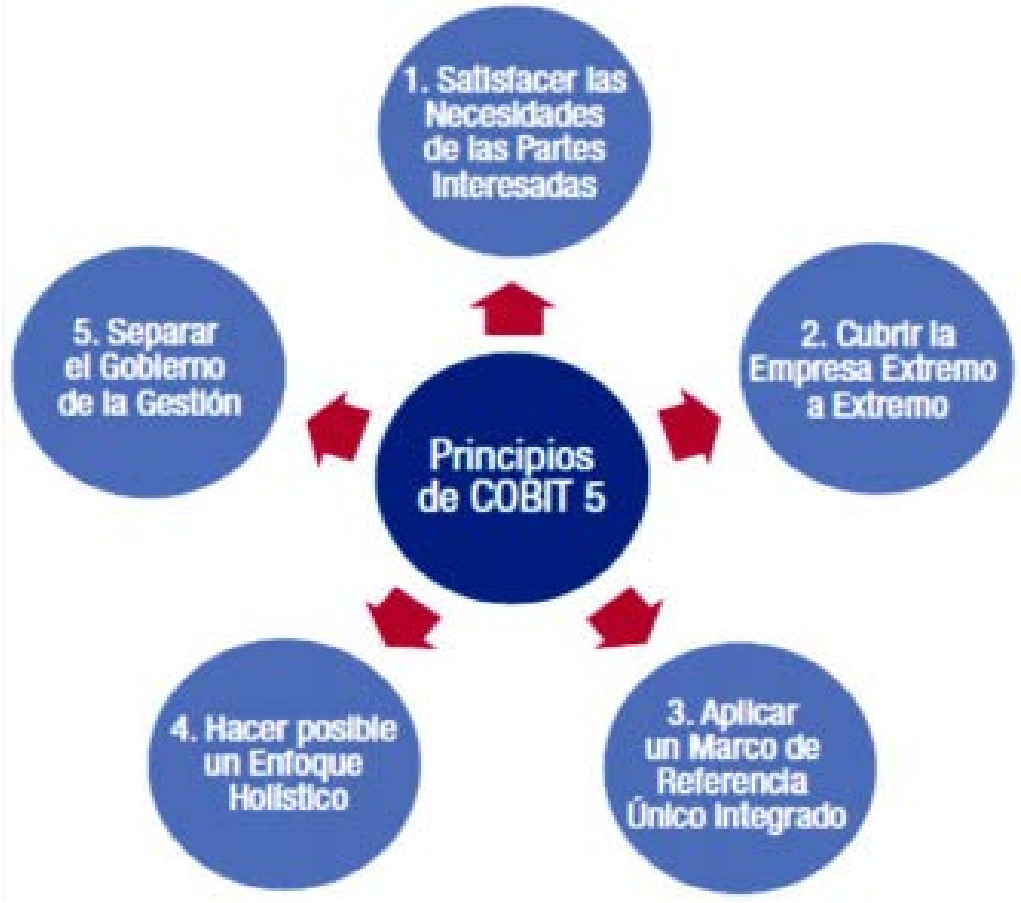


Figura 5-1.

Principios de Cobit 5

Principio 1. Satisfacer las Necesidades de las Partes Interesadas. Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa Extremo a Extremo. COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado. Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico. Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.

- Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

- Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.

- La cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.

- La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.

- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

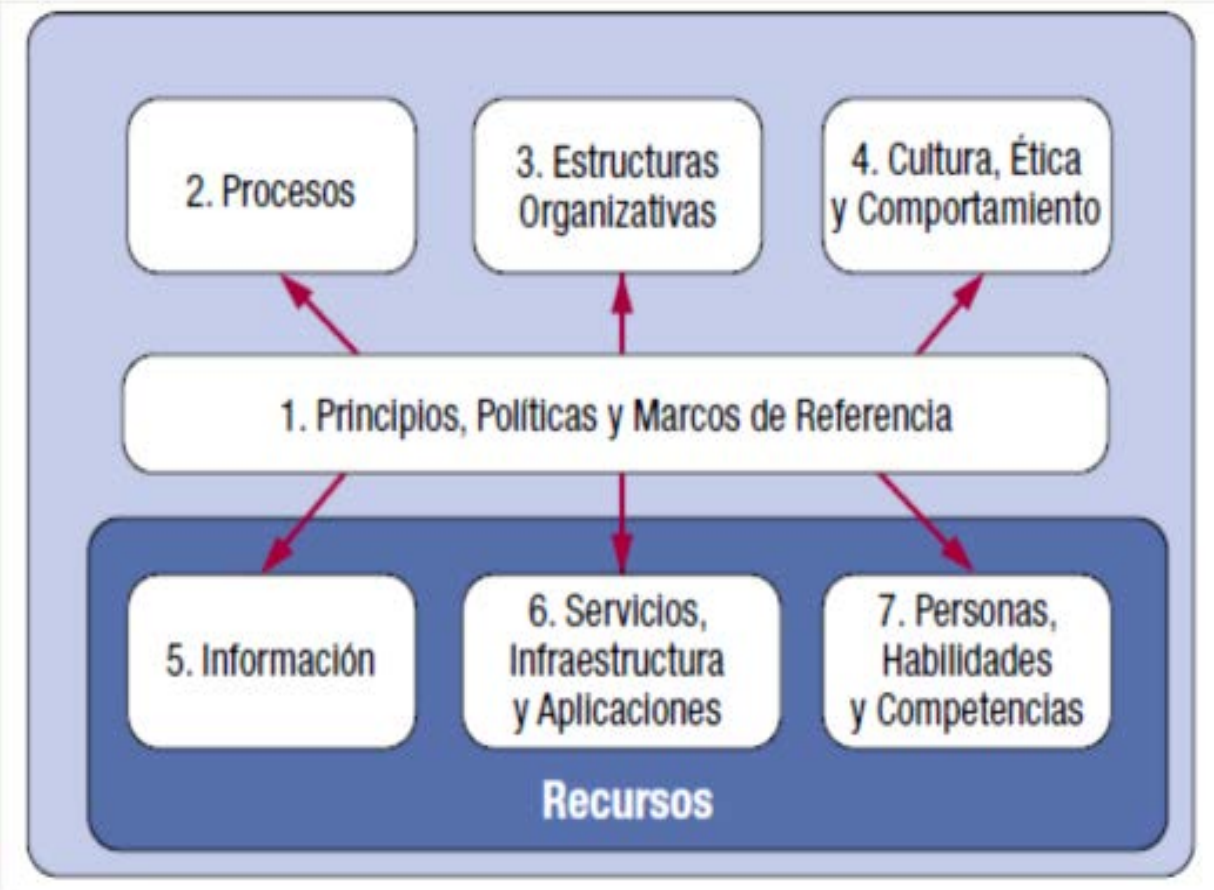


Figura 5-2

Habilitadores de Cobit 5

Principio 5: Separar el Gobierno de la Gestión. El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

- Gobierno: El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

- Gestión: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

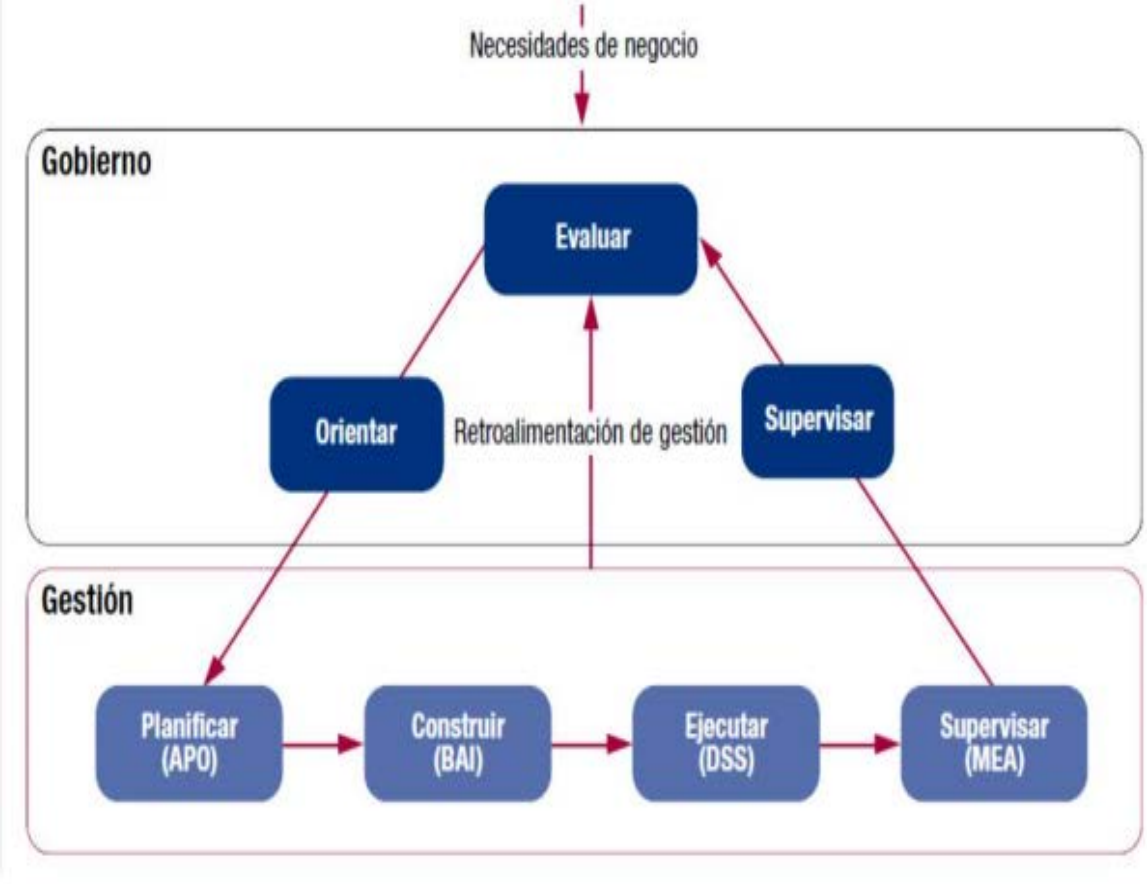


Figura 5-3

Conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5.

Los detalles de todos los procesos, de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía COBIT 5: Procesos Catalizadores.

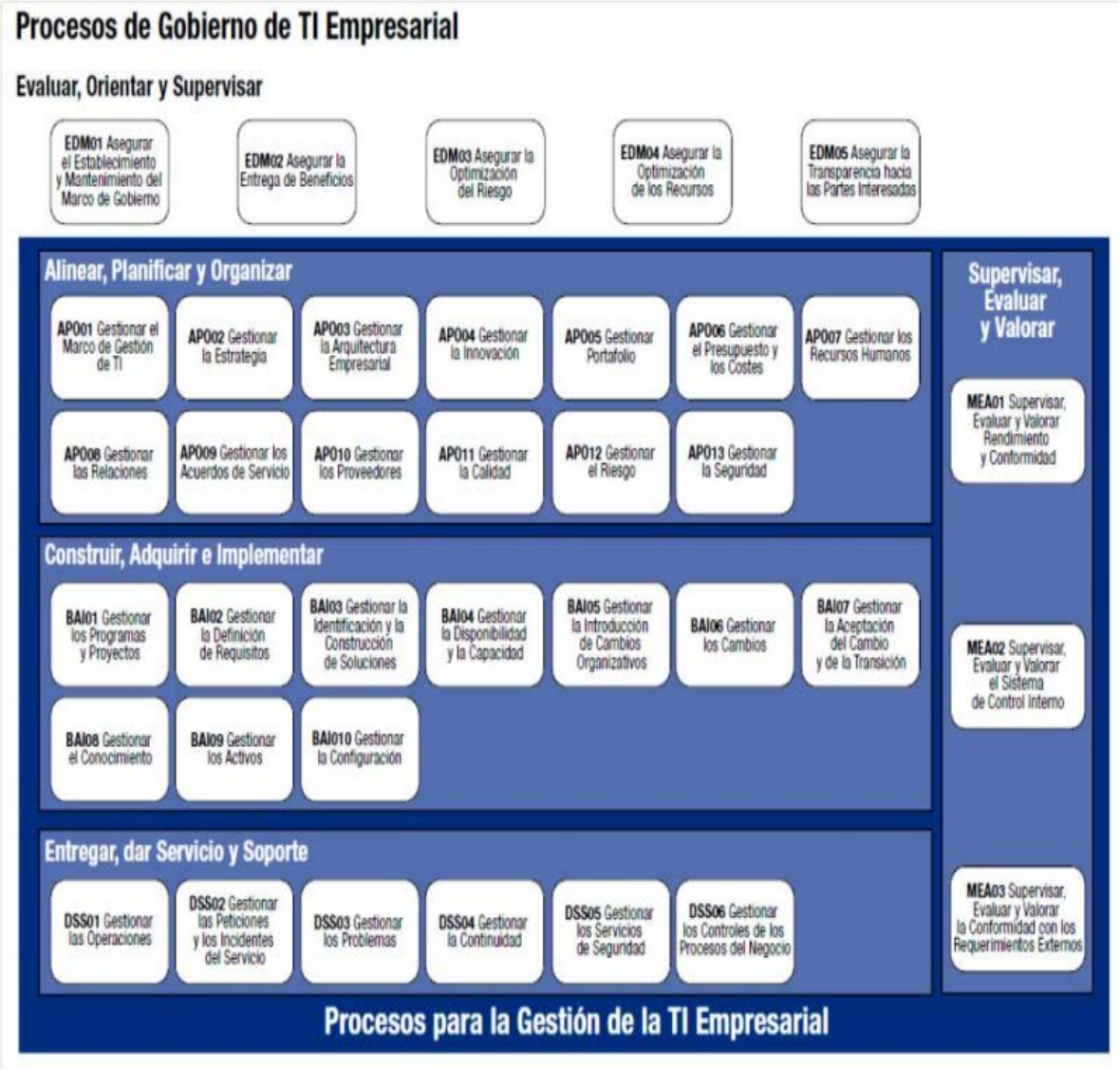


Figura 5-4:

Proceso de gobierno de TI empresarial

5.6 Novedades de Cobit 5

ISACA ha elaborado un documento detallado comparando COBIT 5 con COBIT 4.1 que identifica nueve de las principales diferencias. Para ver el documento completo o solicitar una copia de este documento comparativo, visite el sitio web de ISACA: http://www.isaca.org/COBIT/Documents/COBIT5-Compare-With-4.1.ppt.

Independientemente del documento se exponen aquí algunas de las diferencias más características:

- Al basarse en 5 principios y 7 habilitadores, COBIT 5 utiliza prácticas de gobierno y gestión para describir las acciones que son ejemplo de mejores prácticas de su aplicación. COBIT 5 ha cambiado su enfoque de objetivos de control a una visión por proceso, descripta en detalle por uno de los principales redactores del nuevo estándar, Erik Guidentops, en su artículo “Where Have All The Control Objectives Gone?”

- Se menciona la necesidad de conectarse a o alinearse con otros marcos y normas importantes, como ITIL ®, TOGAF, el Project Management Body of Knowledge (PMBOK), PRINCE2 y la Organización Internacional de Normalización (ISO).

- Se expresa el reconocimiento de que hay muchos usuarios actuales y potenciales que desean centrarse en temas específicos y que tienen dificultades para navegar el material actual e identificar el contenido que va a satisfacer sus necesidades. Cobit 5 refleja esta necesidad general de mejorar la facilidad de uso y la navegación y brinda consistencia en conceptos, terminología y el nivel de detalle necesario.

- El marco actualizado también detalla una matriz RACI más completa para ayudar a aclarar las responsabilidades y proporciona una gama más completa, detallada y clara que COBIT 4.1 sobre los roles genéricos del negocio y de TI. Esto permite una

mejor definición de las responsabilidades de cada rol, o el nivel de participación en el diseño e implementación de procesos.

- COBIT 5 discontinua el enfoque de modelo de madurez de capacidad (CMMI) usado por COBIT 4.1, Val IT y Risk IT. El nuevo enfoque de evaluación de la capacidad del proceso (PAM), se basa en la ISO/IEC 15504 (Spice). Este método es considerado por ISACA como más robusto, fiable y repetible como un método de evaluación de la capacidad de los procesos.

Durante la pasada década, el término “gobierno” ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

5.7 Ventajas

- **Ventajas Cobit 5**
  - Proveer lineamientos avanzados en áreas de alto interés, como la arquitectura empresarial, gestión de activos y servicios y el gerenciamiento de la innovación en Tecnología Información (TI).
  - Cubre la empresa de extremo a extremo. Ya que ayuda a cambiar las visión de los directivos para tomar la responsabilidad de gobernar y gestionar los activos relacionados con TI dentro de sus propias funciones.
  - Ayuda en la satisfacción de los usuarios con los servicios de TI

- **Costos y beneficios**.
  - Adicional mente de los objetivo de gobierno de una empresa se focaliza en optimizar los costos.
  - Gestionar de mejor forma los riesgos (al cuantificar).
  - Explica en forma detallada el modelo de negocio para gestionar la seguridad de la información, invitando a utilizar una perspectiva sistémica

6 ANALISIS COMPARATIVO

En el momento de evaluar la seguridad de los sistemas informáticos (SI) de una organización, o de proceder a la implementación de las políticas de seguridad sobre estos SI, conviene conocer cuál es la terminología que se emplea, cuáles son las áreas en las que se puede aplicar y cuál es el entorno normativo y legislativo en el que nos podemos mover.

En primer lugar se repasan los principales estándares (ISO 27000) y legislaciones, que nos ayudarán a tener una visión global de los elementos que intervienen en la infraestructura de seguridad y los controles que pueden establecerse.

6.1 Conceptos principales en Seguridad de la Información

- Activo (Asset). Algo que tiene valor para una organización. Recurso del sistema de información necesario para el funcionamiento apropiado de la organización y la consecución de los objetivos previstos. Los activos de información pueden estar sujetos a amenazas tanto internas como externas. Estos riesgos pueden afectar a uno o más de los tres atributos fundamentales de un activo: disponibilidad (availability), confidencialidad e integridad.

- Amenaza (threat). Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.

- Confidencialidad (reliability). Hace referencia a la habilidad para proteger, haciéndolos no visibles o no disponibles, los datos de aquellos que no están autorizados a acceder a ellos.

- Disponibilidad (availability). Es la capacidad de poder acceder a los activos informativos en el momento en que se necesiten y de poder usarlos correctamente (aquellos debidamente autorizados).

- Gestión de la seguridad de la información (Information security management) es la parte de la gestión de IT (IT gobernance) encargada de la protección y la seguridad de los activos informativos de una organización (information assets).

- Impacto. Consecuencia para un activo de la materialización de una amenaza.

- Integridad. Es la habilidad de prevenir la modificación de los activos por aquellos que no están autorizados o que estándolo los modifican de forma incorrecta. Esta habilidad implica la posibilidad de revertir o deshacer los cambios realizados.

- ISMS. Information Security Management System. Es la parte de la gestión de un sistema, basada en un análisis de riesgos, encargada de establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información. Un ISMS sirve para asegurar la confidencialidad, disponibilidad e integridad de la información de la organización

- Riesgo. Es la posibilidad de que se produzca un impacto determinado en un activo.

- Salvaguarda (countermeasure). Acción, procedimiento o dispositivo físico o lógico que reduce el riesgo.

- Seguridad de la Información (information security), según el estándar ISO 27001 es la preservación de la confidencialidad, integridad y disponibilidad (availability) de la

información. Otras propiedades implicadas son la autenticidad, responsabilidad (accountability), no-repudiación y confiabilidad (reliability).

- Seguridad, en su sentido más general quiere decir proteger nuestros activos, lo que implica preservarlos de atacantes, de desastres naturales, de condiciones ambientales adversas, de interrupción del suministro eléctrico, del robo o el vandalismo, etc. La seguridad es al mismo tiempo el conjunto de medidas tomadas contra posibles ataques, espionaje, sabotaje, etc.
- Vulnerabilidad. Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.

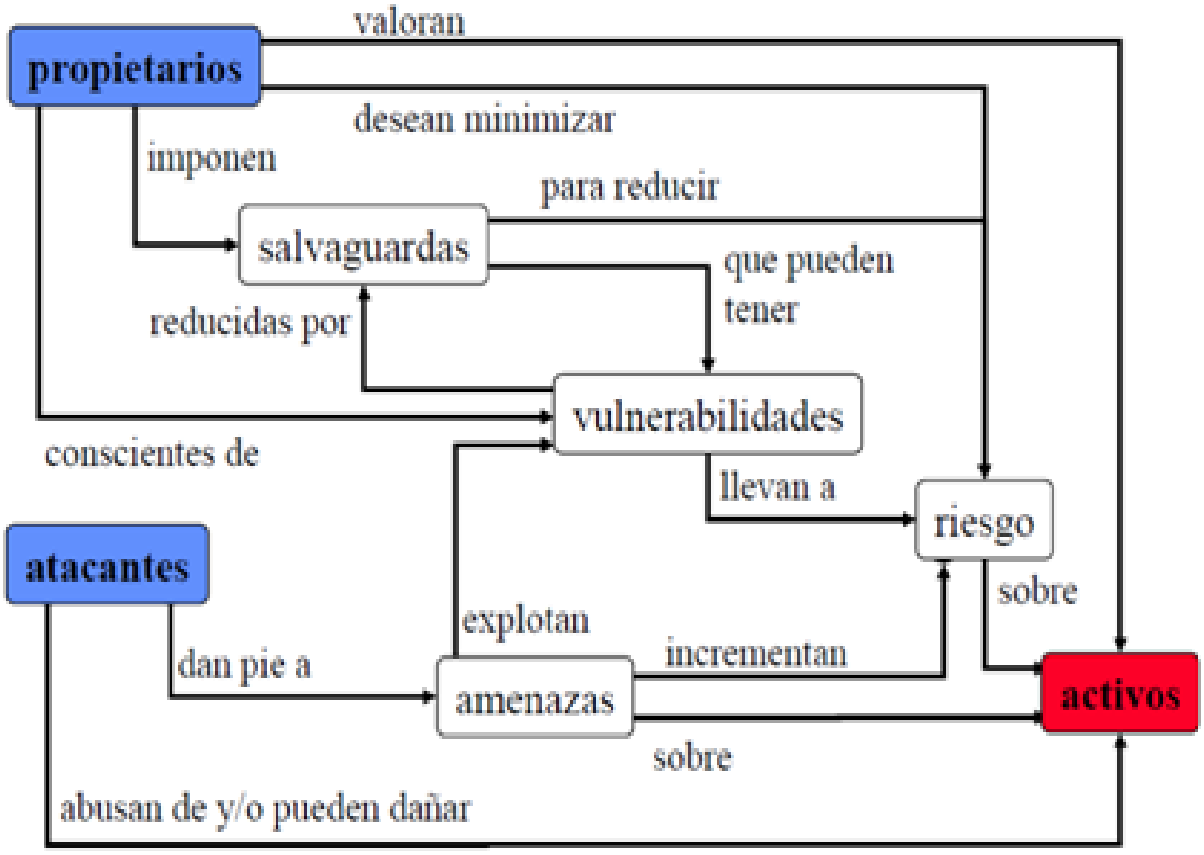


Figura 6-1

Conceptos principales en seguridad y sus relaciones, según ISO 15408.

6.2 Principales organismos dedicados a la seguridad en las Tecnologías de la Información

COBIT (Control Objectives for Information and related Technology). Conjunto de Mejores Prácticas para el manejo de información, creado por Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) en 1992 que contiene un conjunto de 34 objetivos de algo nivel, uno para cada uno de los procesos de IT. La seguridad de los sistemas se divide en objetivos de control, como identificación, autenticación, gestión de cuentas, clasificación de datos, etc. COBIT especifica el examen de la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de los objetivos de control. En el modelo se definen cuatro dominios: planificación y organización, adquisición e implementación, entrega y soporte, y monitorización. Cada uno de estos dominios tienen definidos procesos, actividades y tareas

National Institute of Standards and Technology (NIST, http://csrc.nist.gov). Este instituto gubernamental de USA emite una serie de publicaciones a modo de guías (NIST Guidelines), entre las cuales las más destacadas en relación con la seguridad son las de la serie 800, como: Information Security Handbook: A Guide for Managers (800-100), Recommended Security Controls for Federal Information Systems (800-53), Guide to Information Technology Security Services (800-35), Risk Management Guide for Information Technology Systems (800-30), Engineering Principles for Information Technology Security (800-27), Guide for Developing Security Plans for Federal Information Systems (800-18), Generally Accepted Principles and Practices for Securing Information Technology Systems (800-14), and An Introduction to Computer Security: The NIST Handbook (800-12).

La titulada Security Self-Assessment Guide for Information Technology Systems (800-26), publicada desde el 2001, es una checklist de 137 preguntas para examinar un sistema. La Recommended Security Controls for Federal Information Systems (800-53)

mapea estas cuestiones con los controles de seguridad más utiles. Describe 17 familias de controles, como controles de acceso, sensibilización y formación, auditoría, evaluación de riesgos, seguridad del personal, etc. Cada familia se subdivide en controles específicos que normalmente hacen referencia a otros documentos más específicos del NIST.

Guías de la ENISA. Conjunto de guías generadas por la European Network of Information Security Agency, que busca establecer estándares y difundir Mejores Prácticas para el mejoramiento de las redes y la seguridad de la información en la Unión Europea (Enisa, 2011).

Top 20 de las fallas de seguridad. Presentación anual de los fallos de seguridad informática más críticas hecha por el SysAdmin Audit, Networking and Security (SANS) de los Estados Unidos (SANS, 2011).

OSSTMM (Open Standard Security Testing Model). Manual de la Metodología Abierta de Testeo de Seguridad desarrollado por ISECOM (Institute for Security and Open Methodologies), que brinda una referencia para realizar análisis de seguridad informática en diferentes niveles.

ISM3 (Information Security Management Maturity Model). Estándar para la creación de sistemas de gestión de la seguridad de la información basados en ITIL, ISO27001 o Cobit, a través de metodologías de análisis de riesgo que tienen como objetivo garantizar la consecución de los objetivos del negocio.

ITIL (Information Technology Infrastructure Library). Conjunto de conceptos y buenas prácticas para la gestión de servicios, el desarrollo y/o las operaciones relacionadas con las tecnologías de la información (APM Group, 2007). El conjunto lo constituyen 44 libros. No se dedica exclusivamente a temas de seguridad pero hay una

sección dedicada a ellos e indica cómo implementar controles sobre los procesos de gestión de servicios de IT.

Information Security Forum (ISF) Standard of Good Practice for information Security. Es una guía que contiene un checklist de las políticas que las compañías y empleados deben implementar. Se divide la gestión de la seguridad en 5 partes: aplicaciones críticas para el negocio, instalaciones de computadores, redes, sistemas, y desarrollo. Estas partes se subdividen a su vez en 30 áreas y las áreas en 135 secciones. Las áreas son:

Basel II. Es una compilación del Second Report from the Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking. Estudia y detalla los riesgos de seguridad relacionados con el negocio bancario

Con objeto de harmonizar los diferentes marcos y estándares se elaboró el Calder—Moir IT Governance Framework como una clasificación gráfica que relaciona los principales tópicos como estrategia de negocio, riesgos, estrategia de IT, operaciones, capacidades y gestión de cambios (http://www.itgovernance.co.uk/calder_moir.aspx).

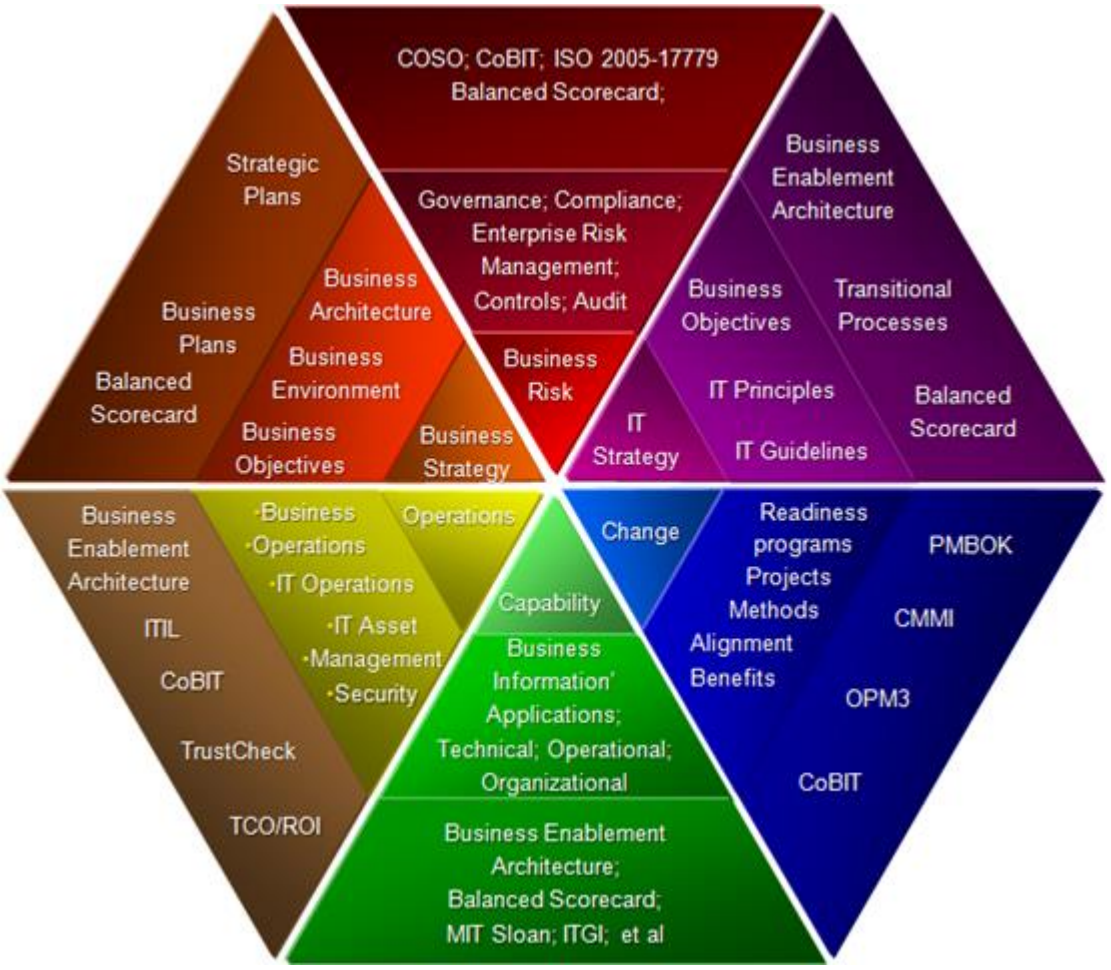


Figura 6-2

Comparativa de áreas contempladas por los diferentes marcos y estándares

6.3 Estándares aplicables

Area	ISO 27000	SAS70 Type II	GLBA	PCI DSS	EU Privacy	CobIT	Common Criteria	Generally Accepted Privacy Principles	Generally Accepted Security Principles
Access Control	X	X	X	X	X	X	X	X	X
Application Development	X	X			X	X	X		X
Asset Management	X	X		X	X				X
Business Operations	X	X		X	X	X	X	X	
Communications	X	X	X	X	X	X	X	X	X
Compliance	X	X	X	X	X	X			
Corporate Governance	X				X	X			
Customers	X	X	X	X	X	X		X	X
Incident Management	X	X	X	X	X	X	X	X	X
IT Operations	X	X	X	X	X	X	X	X	X
Outsourcing	X	X		X	X	X	X	X	X
Physical/Environmental	X	X					X		X
Policies & Procedures	X	X		X	X	X	X	X	X
Privacy	X	X	X	X	X			X	
Security	X	X		X	X	X	X		X

Conclusión

De acuerdo a lo desarrollado en el presente trabajo de investigación, como los objetivos planteados de analizar las dos metodologías que permiten minimizar los riesgos asociados a la seguridad informática tanto internas como externas, así como su potencialidad en la reducción de estas, también en costo-beneficio y el impacto en la gestión. Se concluyó:

- Por razones económicas para las micros y medianas organizaciones OSSTMM es el que mejor se aplica en estos lugares. Debido principalmente a las dificultades de precio que Cobit tiene.
- OSSTMM está orientado a la seguridad informática y otros aspectos más generales.
- En esencia Cobit está orientado al negocio de TI.
- Para las grandes empresas Cobit 5 se ajusta, ya que es una inversión en la reducción de los costos en seguridad y cuentan con el recurso económico para solventar las versiones actuales y venideras de Cobit.

GLOSARIO

BUCLE

Un bucle es utilizado para hacer una acción repetida sin tener que escribir varias veces el mismo código, lo que ahorra tiempo, deja el código más claro y facilita su modificación en el futuro.

DDoS

En seguridad informática, un **ataque de denegación de servicios**, también llamado ataque **DoS** (siglas en inglés de *Denial of Service*) o **DDoS** (de *Distributed Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

FREEWARE

Free (gratis) ware (software). Cualquier software que no requiere pago ni otra compensación.

HTTP

Hypertext Transfer Protocol o HTTP (en español *protocolo de transferencia de hipertexto*) es el protocolo usado en cada transacción de la World Wide Web.

ITIL

La Biblioteca de Infraestructura de Tecnologías de prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

OPEN SOURCE

Código abierto es la expresión con la que se conoce al software o hardware distribuido y desarrollado libremente. Se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre. Para muchos el término “libre” hace referencia al hecho de adquirir un software de manera gratuita, pero más que eso, la libertad se refiere al hecho de poder modificar la fuente del programa sin restricciones de licencia, ya que muchas empresas de software encierran su código, ocultándolo y restringiéndose los derechos a sí misma.

SNIFFING

Se trata de dispositivos que permiten al atacante “escuchar” las diversas comunicaciones que se establecen entre ordenadores a través de una red (física o inalámbrica) sin necesidad de acceder física ni virtualmente a su ordenador.

TELNET

(***Tel****ecommunication* ***Net****work*) es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

BIBLIOGRAFIA

Papel

1. COBIT. Control Objectives for Information and Related Technology

2. Carnegie Mellon University. Ingeniería del Software, Seguridad informática

3. FAST: Federation Against Software Theft, servicios para prevenir el uso de software ilegal. 1984.

4. GAISP: Information Systems Security Association, principios y buenas prácticas recomendadas en Seguridad de la Información.

5. SANS Institute (SysAdmin Audit Networking and Security Institute), seguridad en redes.

6. NIST. National Institute of Standards and Technology, agencia no regulatoria del Departamento de Comercio de US, Promover la seguridad mediante tecnologías, metrologías y estándares.